pwc

Unified Fintech Forum
POWERING RESPONSIBLE FINTECH

Privacy in digital India: The road from Viksit to Surakshit Bharat

Foreword from UFF

Jatinder Handoo
CEO
UFF

India's digital transformation has been nothing short of extraordinary. In just a few years, technology has fundamentally changed how we pay, borrow, save, invest, and interact with businesses and government. What was once considered digital innovation has now become part of everyday life for millions of Indians. As AI, embedded finance, and digital public infrastructure continue to reshape our economy, another equally important conversation has emerged—the conversation around trust.

Trust has always been the foundation of financial services. In the digital era, that trust is increasingly built on how responsibly organisations collect, use, protect, and govern personal data.

The Digital Personal Data Protection Act (DPDPA) marks an important milestone in India's journey towards a mature digital economy. Yet, privacy cannot be achieved through legislation alone. It requires organisations to rethink their approach to technology, governance, and customer relationships. Privacy should no longer be viewed as a compliance exercise that is addressed after products are built. Instead, it must become an integral part of innovation itself. This is especially relevant for the FinTech and BFSI sectors. Financial institutions today rely on data to deliver faster credit, detect fraud, personalise customer experiences, and power intelligent decision-making. AI is accelerating these possibilities even further. However, considering such a wide array of capabilities, it is more important than ever to ensure responsible practices. Organisations must now ensure that innovation is accompanied by transparency, accountability, and responsible data practices that inspire confidence among customers and regulators alike.

The objective of this report is not merely to explain the evolving privacy landscape. It is to encourage a broader dialogue on how India can continue to lead the world in digital innovation while strengthening the safeguards that protect individuals and businesses. The report brings together perspectives on emerging technologies, regulatory developments, sectoral implications, and global trends, while highlighting the opportunities that arise when privacy is embedded into business strategy rather than treated as an afterthought. At the Unified Fintech Forum, we believe India's FinTech ecosystem has consistently demonstrated its ability to innovate responsibly. The same collaborative spirit that enabled the growth of digital payments, lending, account aggregation, and other digital public infrastructure will now be essential in creating a privacy-first digital economy. Policymakers, regulators, technology providers, financial institutions, and consumers all have an important role to play in building this shared future.

Importantly, privacy should not be seen as a barrier to growth. Organisations that earn customer confidence through ethical data practices will be better positioned to innovate, attract investment, and build enduring relationships. In the years ahead, competitive advantage will increasingly belong to enterprises that combine technological excellence with responsible governance.

I congratulate PwC India and everyone associated with this publication for developing a thoughtful and timely report on an issue that will define the next phase of India's digital journey. I hope the insights presented here encourage meaningful conversations, informed decision-making and collective action towards creating a digital ecosystem that is innovative, inclusive, secure, and trusted by every citizen.

Message from PwC

Amol Bhat
Partner, Leader – Cyber and Digital Risk (Financial Services)
PwC India

Our generation is witnessing a defining moment in the digital age. Technologies such as AI, IoT, cloud computing, and advanced analytics are transforming the way we live, work, and conduct business. These innovations are not just unlocking new opportunities but also reshaping one of the most fundamental expectations of the digital era—privacy.

As we transition from a physical to a digital era, the concept of privacy has also evolved. Our focus has expanded from safeguarding physical spaces—such as homes, offices, and personal records—to protecting digital spaces, including online identities, financial information, health data, and personal communications. While this describes a fundamental shift, it also captures the growing importance of data privacy in modern society.

For the financial services and FinTech sectors, this responsibility has become even more important. As custodians of sensitive customer and financial information, these institutions are operating under constant pressure from regulators, customers, and competitors.

The DPDPA marks an important milestone in India's digital journey. More than a compliance requirement, it presents an opportunity for organisations to embed privacy into every fabric of their business to strengthen governance, enhance transparency, and reinforce customer confidence.

This report explores the evolving data privacy landscape in India through the lens of DPDPA and rise of emerging technologies. It examines the challenges and opportunities presented to financial institutions and enterprises as they balance innovation with accountability.

As India continues its digital transformation, our collective success will depend not only on how rapidly we innovate but on how responsibly we manage data.

I would like to thank my colleagues from the UFF for contributing their valuable insights to this report.

Contents

01

Introduction

India's digital economy is booming at nearly twice the pace of the overall economy and is projected to account for around one-fifth of the GDP by 2026–2030, driven by platforms such as UPI, e-commerce, AI-enabled services, and Aadhaar-linked digital ecosystems.[1] As digitalisation becomes more deeply rooted across financial services and our daily transactions, individuals' digital footprints are also rapidly expanding. This has increased the volumes of personal and behavioural data being captured through UPI payments, Aadhaar-based authentication, mobile applications, and embedded financial platforms. This structural and transformational shift has made data a core economic pillar and growth driver, while also amplifying the risks pertaining to privacy, regulatory expectations, and systemic impacts on FinTechs and financial institutions.

The Digital Personal Data Protection Act (DPDPA) is not just a data protection checklist. It also establishes a horizontal, technology-neutral framework for personal data processing in India that applies across sectors, including BFSI and FinTech. The act has arrived at a point when digital payments already account for over 99.8% of the nation's retail transaction volume[2] and UPI processes more than 23 billion transactions in a month,[3] embedding privacy-related risk deeply into our everyday financial activities.

Consumers increasingly say privacy matters, and over 80% of Indian consumers consider protection of personal data to be a critical element to trust, but only 16% report understanding the nitty-gritty of the DPDP Act, highlighting a significant gap in awareness and literacy.[4] Globally, India's regime converges with high-penalty global privacy models such as EU's GDPR, while also experimenting with an India Stack-style digital public infrastructure, consent managers, and AI-driven data governance.

For large FinTech organisations and financial institutions, the DPDPA is not just a compliance obligation but a strategic inflection point that will reshape product design, AI use cases, data monetisation strategies, cross-border architecture, and incident response playbooks. This report explores that landscape, with a focus on new-age financial sector technology.

1 https://www.pib.gov.in/FactsheetDetails.aspx?Id=149096&reg=3&lang=2
2 https://bfsi.economictimes.indiatimes.com/news/fintech/digital-payments-dominate-retail-transactions-in-india-in-q1-fy26/124524010
3 https://www.aninews.in/news/business/upi-hits-new-high-in-may-2026-with-232-billion-transactions-worth-rs-299-trillion-npci-data-shows20260602155337/
4 https://www.pwc.in/press-releases/2024/82-of-indian-consumers-consider-protection-of-personal-data-as-most-crucial-factor-in-building-trust-pwcs-voice-of-the-consumer-survey-2024.html

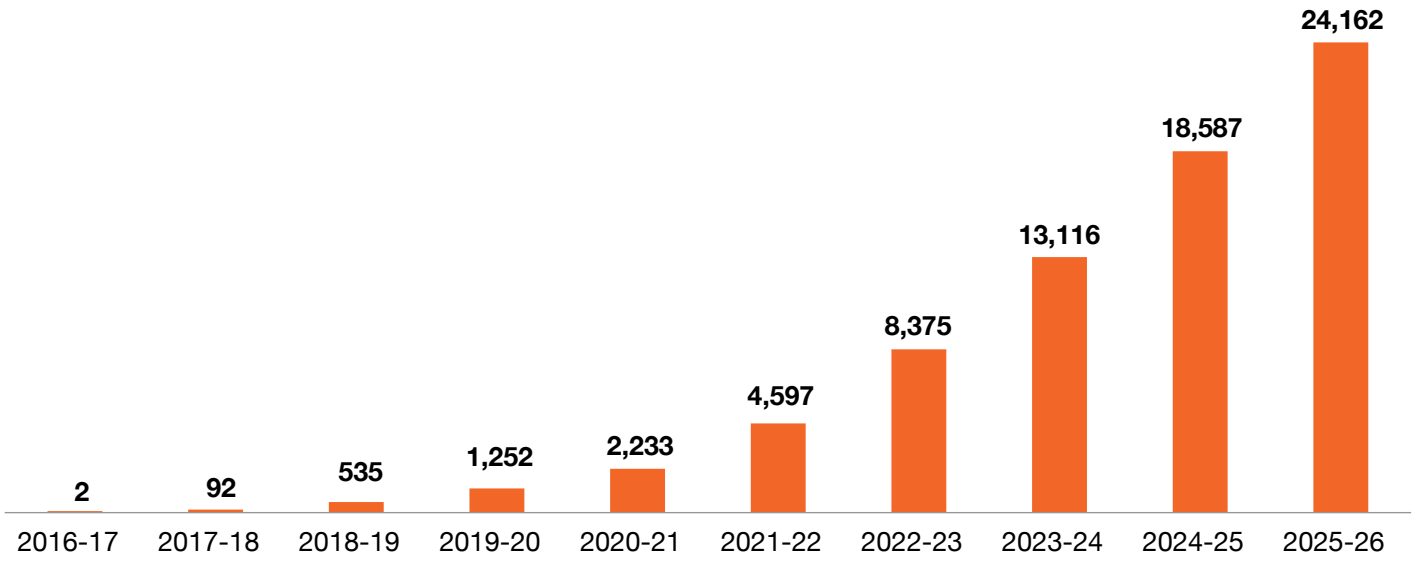
02

The digital India Stack: Economy, security, and next-gen tech

2.1 India's digital economy growth

Government and independent estimates placed India's digital economy at around 11–12% of GDP in 2022–2023, and projected it to grow to about 20% of gross value added by 2029–2030. Digital-first sectors such as information and communication technology, electronics manufacturing, and digital platforms such as UPI, Aadhaar etc. have been growing by around 17% every year for the past decade, compared with overall economic growth.[5]

Figure 1: UPI financial transaction volume



Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2257087&reg=3&lang=2

Digital payments are one such use case. In FY 2025–2026, UPI processed more than ₹24,000 crore (241.6 billion) transactions valued at around ₹314 crore, in which over 23 billion transactions were processed every month in 2026. Digital channels accounted for 99.8% of retail payments by volume and 92.6% by value in Q1 FY2026, implying that paper-based payment modes have almost been eliminated in the country.[6,7]

5 https://www.pib.gov.in/FactsheetDetails.aspx?Id=149096&reg=3&lang=2
6 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2257087&reg=3&lang=2
7 https://bfsi.economictimes.indiatimes.com/news/fintech/digital-payments-dominate-retail-transactions-in-india-in-q1-fy26/124524010

2.2 Rise of FinTech, e-commerce, and AI

The rise of FinTech companies, neobanks, lending platforms, and insurance technology (insurtech) is enabled by UPI, Aadhaar, digital KYC processes, account aggregators, and embedded finance, with end credit. India is a front-runner in AI adoption. A digital economy index, published in an ICRIER report, placed India at the fifth position in overall digitalisation up from the eighth place in 2025 and fourth in the AI CHIPS index, just behind the US, China, and Singapore.[8]

This ecosystem is becoming increasingly data-intensive, determining scores with alternative data, fraud checks with machine learning algorithms, hyper-personalised product offers, robo-advisory services, and chatbots driven by generative AI (GenAI). These capabilities present new privacy challenges—ranging from continuous behavioural profiling to the application of data in different contexts and the use of opaque algorithms.

2.3 Privacy–security imperative for India's digital economy

An interesting fact about the present state of cybersecurity in India that makes risk so noteworthy is the scale of digital transformation. More than 2.2 million cybersecurity incidents occurred in India between 2021 and 2025, roughly accounting for more than 3,000 cyberattacks daily. This makes the BFSI sector one of the most continuously attacked sectors (e.g. cyberattacks on India's leading cryptocurrency exchanges, Aadhaar systems etc.).

Consequently, the Indian industry has spent an average of ₹19.5 crore on incurring a cyberattack, and AI cybersecurity risks are also becoming critical and noteworthy with model poisoning, prompt injection, and phishing chatbots. New regulations such as the DPDPA impose consent, processing limitations, and accountability, making India one of the hardest countries to operate in regarding future cybersecurity issues.[9,10]

8 https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2026.pdf

9 https://www.techcircle.in/2025/10/29/india-s-digital-boom-faces-a-cybersecurity-reckoning

10 https://news.fundsforngos.org/2026/05/25/indias-5-trillion-economy-ambition-faces-rising-cybersecurity-risks-experts-warn/

03

From the IT Act to the DPDPA: India's road to privacy

Privacy is not a new concept—even in medieval times, individuals used to ensure privacy by creating physical boundaries like solar rooms and seclusion of religious figures in everyday life. In the digital age, privacy concepts have shifted from physical boundaries to protecting personal digital data, which has become increasingly important in the modern world due to the pervasiveness of AI and technological connectivity. As such, it has evolved from a social norm to a fundamental human right and an economic necessity.

1998 – IT Action Plan
The Prime Minister's Task Force on Information Technology recommended that steps be taken to protect citizens' digital information. The task force's recommendation of a national policy on information security and a national data protection law was India's first official recognition of the need to develop formal data privacy policies.

2000 – IT Act
The IT Act, 2000 formulated a legal framework for financial data safety, cybercrimes, and electronic commerce. The act was not precisely a privacy law per se but provided India's first legal framework for regulating electronic information.

2011 – SPDI Rules
The Sensitive Personal Data or Information (SPDI) Rules were issued under the IT Act, which governed sensitive personal information and applied to corporate bodies or any person located in India.

2012 – Justice A.P. Shah Committee
The committee's report captured nine core privacy principles, including informed consent, purpose limitation, and accountability. These core principles influenced India's data protection laws.

2017 – Justice K.S. Puttaswamy v. Union of India
In a landmark judgement, a Supreme Court ruling acknowledged that privacy as a fundamental right enshrined in the Constitution's Article 21. This ruling laid a foundation for India's data protection regime.

2018 – Justice Srikrishna Committee
The committee recommended India's first comprehensive personal data protection (PDP) framework and presented a draft law. In addition, their proposals established the basis for subsequent drafts.

2019 – Draft PDP Bill
The bill proposed a comprehensive PDP framework. It also recommended the establishment of a Data Protection Authority and gave citizens the right to data portability and the right to have data erased. The bill was introduced to the Parliament but withdrawn in 2022 for further revisions.

2023 – DPDP Act
The DPDP Act is India's first legislation to regulate digital personal data. The law detailed a consent-based framework for data processing and data principals' rights and imposed obligations on data fiduciaries.

2025 – DPDP Rules
The DPDP Rules are operational instructions for implementing the DPDP Act that enforces a detailed procedure for notices and consent, directions for personal data breach notification, and guidance for data fiduciaries.

04

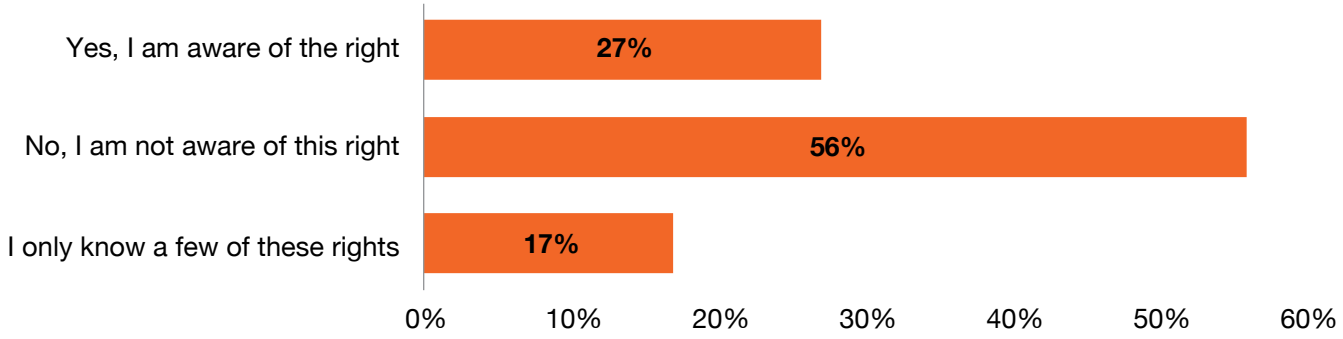
Consumer awareness and digital literacy

4.1. Current state of privacy awareness

Indian authorities have recognised and actively addressed the need for data privacy, addressing it through legal frameworks. Despite all these efforts, consumer understanding regarding the data protection law remains low. According to a PwC report, only 16% of Indian consumers indicated that they understood the DPDP Act.

The report also revealed that approximately 82% of Indian consumers considered personal data protection to be the most important factor in building consumer trust.[11] The report also emphasised that consumer awareness of data rights related to personal data stands at 56%.

Figure 2: User awareness of the right to have personal data deleted if desired



Source: How aware and prepared are Indian consumers and businesses to navigate the new era of digital privacy? - PwC

4.2. Digital literacy and attitudes towards personal data

Although digital literacy in India has improved considerably due to the rise of smartphones and internet use, it has not linearly translated to data privacy awareness as consumers are still unfamiliar with privacy notices, risk disclosures, and consent.

A PwC survey found that 83% of the Indian respondents wanted their devices to protect their personal data and keep it private. Conversely, two-thirds of the respondents were also willing to share data with companies that offer discounts or rewards and less wary about cross-sharing data between social networks or using data for reasons they are unable to identify.[12]

11 https://www.pwc.in/press-releases/2024/only-16-consumers-in-india-understand-the-digital-personal-data-protection-dpdp-act-only-9-indian-organisations-report-a-comprehensive-understanding-of-the-act-pwc-india-survey.html

12 https://www.pwc.in/press-releases/2024/82-of-indian-consumers-consider-protection-of-personal-data-as-most-crucial-factor-in-building-trust-pwcs-voice-of-the-consumer-survey-2024.html

05

The next risk frontier: Privacy and emerging technology

5.1. FinTech: Personalising finance

FinTech companies use transaction data, customer analytics, and user device details to enhance credit scoring, detect fraudulent activity, and offer a customised financial services experience. Research conducted across multiple countries across the globe has indicated that open banking initiatives that enable financial information sharing between entities positively influence and promote FinTech development. Nevertheless, increased customer data accessibility to third parties creates privacy and security concerns. The question whether personalisation is useful also depends on how consumer consent is established—which should be explicitly, unambiguously, and transparently taken—particularly in the context of the rapidly evolving digital world.

Scenario: Account aggregation and hyper-personalisation

A personal finance app aggregates and analyses data across multiple accounts, highlighting spending patterns and providing consumer insights. By analysing these patterns, the app can segment users into different categories such as those with 'high incomes and high discretionary spender' or 'low income and frequent defaulters'.
The same information can be used to infer customers' disposable incomes, attitudes towards other essential considerations such as health and education spending and risk appetites, which can be used for cross-selling to finance companies that seek to lend to or insure these segmented groups. However, bundled and opaque consent can introduce consumer protection concerns if customers are not aware of how their data will be used, and this aggregation of personal data can lead to privacy violations.

5.2. Cloud computing: Where confidentiality meets cloud-scale risk

Cloud computing is the backbone of many FinTech and BFSI workloads. It provides flexibility and scalability and stores vast amounts of customer data in shared environments managed using scripts and inherent cloud settings. It is seen that misconfigured storage systems and services are among the leading causes of cloud security incidents. Research and post-incident analysis has clearly demonstrated that most cloud breaches incidents were caused by misconfigured storage buckets or services with overly permissive settings.[13] These lapses have resulted in exposing customers' sensitive personal and financial data to anyone on the internet.

Use case: Misconfigured storage

Analyses of security incidents pertaining to cloud storage have revealed a few recurrent themes, which are often attributed to similar misconfigured storage. One of these is the presence of an open or improperly configured object storage, resulting in the leakage of millions of sensitive customer records. In such a scenario, a FinTech company that is using cloud storage to store data pertaining to loan applications could have customer data exposed due to misconfigured cloud storage and can also attract regulatory fines and rule-based penalties.[14]

5.3. Payment ecosystems: Invisible trails in real-time transactions

The digital payment ecosystem, which includes UPI, wallet, and cards, not only makes everyday life convenient but also leaves a digital footprint, including the sum of money being transferred and transaction details capturing where, when, and how a customer spends, their devices, and their locations. These data may be mined to build behavioural profiles. Individually, the details or data seem inconsequential; however, when seen together, they create a compelling picture of customers' likes, needs, and desires. While banks and payment providers use this information for fraud prevention, they increasingly use these data for customer profiling and targeting. Few consumers are aware of the extent of their personal data being mined and used for unknown purposes.

Use case: The profile behind every payment

We tend to not think about the details when paying for our morning coffee, a cab ride to the office, groceries, a charity donation, or even an online purchase. The details of these transactions softly reveal users' lifestyle, schedule, and even ideology. Aggregators—such as payment apps and websites and the banks themselves—collate and analyse these data segmented users in different category pools such as frequent traveller, health enthusiast, etc. and present credit card offers to target users based on where and how they spend. While these practices may be prevalent, this approach can go beyond targeting to interfering with customers' privacy and choices, potentially violating India's DPDPA and other data protection laws.

13 https://www.cloudcomputing-news.net/news/misconfiguration-was-the-number-one-cause-of-cloud-security-incidents-in-2021/
14 https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

5.4. Blockchain: The paradox of public ledgers

Public blockchains are often touted as inherently anonymous, but it is also seen that users can be de-anonymised by analysing blockchain data such as transactions and addresses to real identities. Additionally, the study emphasises that any financial flow and interaction data stored on a public ledger are permanent and irrevocable, leaving a 'digital footprint' that is difficult to remove. Unlike the centralised databases used by banks, where financial transactions records can be deleted or adjusted depending on specific regulations, blockchain does not provide such flexibility and introduces serious privacy concerns.

Use case: Tracing crypto transactions

Individuals may use crypto to fund NGOs, pay for journal subscriptions on sensitive topics, or purchase any online service, believing that blockchain anonymity will protect their identity and keep their transaction private. However, research companies can possibly analyse this data, group it together with other data points such as addresses and transactions, and identify the target's exchange or business, from where the funds were cashed out. Even after decades, these transaction records have the potential to reveal user preferences as well as the NGOs the target was supporting, the journals they were interested in, and other personal details, becoming a grave privacy concern.

5.5. IoT: From sensors to surveillance

The world is more connected today with a myriad of connected devices at home, in factories, around the cities—silently gathering information about our identity, activities, location, biometrics, and even about our environment without any restriction. Many such devices even collect personal and invasive information such as identifying who is at home, when and how they arrived, and what they do there—including what they say and how they feel. Together, such data can form a comprehensive picture of people's lives. These details are of great value to these manufacturers and cloud providers as they can monetise them.

Use case: The listening living room

Smart speaker, car IoT devices, and other digital capabilities are used in daily life, involving user commands that can be referenced to improve suggestions. Aggregating these data can help build a profile of users' interests and political, religious, or health views. Additionally, if these details are considered holistically, companies can determine when people are at home, when they leave, and even when they plan to go on vacation. In essence, individuals' privacy can be severely compromised by these connected devices turning into analytics labs, with few entities understanding or even accessing these data.

5.6. Digital healthcare

Digital health technologies offer a convenient and faster way to deliver healthcare using video consultations, e-pharmacies, smart wearable sensors, and health apps. However, in the background, these healthcare solutions often include individuals' highly sensitive health data, which could include diagnoses, test results, mental health or fertility treatment records, and even lifestyle data. Comparative studies of telemedicine frameworks have revealed and highlighted that India's laws have not treated personal health information (PHI) with the same importance as seen in other parts of the world, even though the world is moving more towards mobile and cloud platforms.[15]

Use cases: Telehealth consultation platforms

A patient has an intimate conversation with a doctor about a personal health crisis or any family triggers via telehealth consultation, confident that this discussion will remain private and secure. However, the teleconsultation platform may be using these recorded sessions to improve the quality of care by contributing to training files for triage algorithms and developing new wellness products. The patient who only opted for a telehealth consultation may have unknowingly become part of these training data. Even if the data are not deliberately shared, their use can be perceived as a breach of confidentiality if not disclosed upfront or obtained without consent.

15 https://pmc.ncbi.nlm.nih.gov/articles/PMC10048681/#abstract1

5.7. Smart homes: Walls that listen

Smart homes offer new-age solutions to modern problems, enabling users to lock or unlock doors, control lights and other equipment, alerting possible break-ins, and having appliances and systems communicate with each other. However, this level of comfort and convenience can be hindered by privacy breaches as these devices gather information from users' day-to-day lives. Smart home products analyse and share the telemetry with manufacturers and big cloud companies, with little information provided about what data are shared and how. The sad truth is that all of this can be executed without due consent and transparency.[16]

Use case: Intrusive smart home devices

Smart home security devices, such as Amazon's Ring video doorbell and camera, have already demonstrated the potential to be abused. Amazon's Ring has been openly criticised for having partnerships with thousands of police departments and sharing video evidence with the police without users' knowledge or consent. Although the ability to request videos directly from the Ring app was removed from the Pro plan, law-enforcement agencies still exercise the power to request these details via warrants or directly from the court.[17]

5.8 Robotics: Machines that see, hear, and remember

Advancements in robotics are getting increasingly prevalent across various industries such as healthcare, logistics, warehousing, and even hospitality. Robots often require cameras, microphones, and other sensors to navigate and interact effectively with their environment, implying that these bots are continuously capturing images and sounds as a by-product of their operation, including personal identifiable information. Researchers and analysts have argued that such robots should be more privacy aware and 'know' when not to look or listen by being cognisant of human privacy in terms of information capture and subsequent behaviour modification based on the contextual space.

Use cases: Curious case of carebots

A hospital that deploys robots to carry medicines and lead visitors around the facility is likely to equip the robot with cameras and depth sensors to navigate the environment while avoiding obstacles, including humans. The robot would also be equipped with microphones to respond to verbal commands and queries and record information for 'service improvement' purposes. As a result, the robot will capture geographical details of the individuals within closed rooms and private verbal interactions that may occur within its auditory range. By virtue of being able to record and store these data, the robot is a security risk, particularly when the data are used beyond the intended purpose. A privacy-aware robot would ensure that it does not record or delete data and provide context-based information about its surroundings to humans, making it safe.

16 https://www.newsnationnow.com/business/tech/ring-doorbell-cameras-privacy-safety/
17 https://www.bbc.com/news/articles/cwy8dxz1g7zo

06

Convergence of AI and privacy: Data, decisions, and trust

AI has become the decision engine in the modern digital world that is able to spot fraud, route payments, produce credit scores, draft communications, and run chatbots with speed that surpasses human capabilities.

What is privacy in the age of AI? It is not merely a matter of one data point versus many but information that computers can glean about us, how that information might be used, and our sense of control over these processes.

6.1 AI: Building walls without trust

The world is engrossed in a global AI arms race and a battle to achieve AI dominance. Advanced economies and leading AI research companies (e.g. OpenAI and Anthropic) are racing for the first place to achieve artificial general intelligence and artificial superintelligence. Companies and governments participating in this race are also completely focused on achieving dominance, rendering data and security insignificant in the process.

Both AI adoption and concerns about its use are rising rapidly. According to the Stanford AI Index Report 2026, GenAI reached 53% population adoption within just three years, making it one of the fastest-adopted technologies in history. Additionally, 88% of organisations reported using AI for day-to-day workplace activities. However, trust remains a significant challenge, with 52% of people expressing concerns about AI, particularly regarding the collection and sharing of personal data.[18] People are using GenAI platforms, entering personal or confidential data, including financial and medical information, into these systems. There is an apparent gap between AI use and privacy as people use GenAI platforms for ease and convenience but do not understand how their data are processed in these systems and where data are shared.

In general, people want to engage with AI and they are willing to accept this technology in their everyday lives if the organisations that use their data prioritise transparency and provide them with the ability to control how their data are used.

18 https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf

6.2. How financial services are using AI with privacy at the core

India's AI market was valued at $9.51 billion in 2024, grew to $13.05 billion in 2025, and is projected to reach $130.63 billion by 2032, registering a compound annual growth rate (CAGR) of 39% during the forecast period.[19]

These numbers set expectations of AI having a pivotal influence on BFSI and other sectors in the next 5–7 years. Leveraging AI to obtain transformational value in operations, compliance, risk management, and customer experience will make the banking sector a real growth engine.

The finance industry's adoption of AI reaches beyond experimentation. An industry survey revealed that 57% of respondents had already implemented AI for data analytics, making it the most adopted application, followed by GenAI as the second most used technology.[20]

The rapid AI adoption has attracted privacy concerns into these conversations. Supervisory bodies and other regulators are emphasising the following concerns:

- **Data supply chain visibility** – Data supply chains are a critical concern, spanning data provenance and lineage, storage and reuse of data used to train AI models, and the application of new data across different systems and models.
- **Explainability and fairness** – These concerns are gaining importance as firms grapple with the need for transparency and providing rationale to customers and regulators for the decisions made by AI systems that include the use of personal data.
- **Vendor and third-party risk** – With the increased use of third-party technologies, vendors' and partners' approaches to data privacy and security are also coming under increased scrutiny.

Privacy considerations cannot be delinked from BFSI and FinTech firms' AI strategy. Data protection and chief AI officers must work collaboratively and closely on data governance, model governance, customer communications, and other important matters.

6.3. AI as a privacy risk and privacy tool

Emerging research has indicated two ways in which data privacy can be impacted by AI. First, it can negatively impact privacy by enabling more intrusive profiling, re-identification of de-identified datasets, and reverse engineering of sensitive information. For example, models may infer private details about an individual from behavioural, transactional, or social data—even when the information was not deliberately shared. This highlights the importance of minimising data collection, using information responsibly, considering the context in which it is handled, and being aware of the risks associated with algorithmic recommendations.

Second, privacy can be protected and even enhanced using AI using techniques like federated learning, differential privacy, and AI-powered access control. Using such methods, companies can analyse aggregated data on fraud detection or credit scoring without compromising individuals' privacy. In the financial service space, AI can inform product design such as fraud detection platforms. Therefore, by design, while AI may introduce new privacy threats to, it can also help prevent or mitigate them.

19 https://www.pwc.in/industries/financial-services/ai-in-indian-banking.html

20 https://www.statista.com/statistics/1374567/top-ai-use-cases-in-financial-services-global/

6.4 Insights for AI–privacy convergence

Considered holistically, data points clearly indicate a strong and powerful insight wherein **trust in AI and trust in privacy** have become two sides of the same coin.

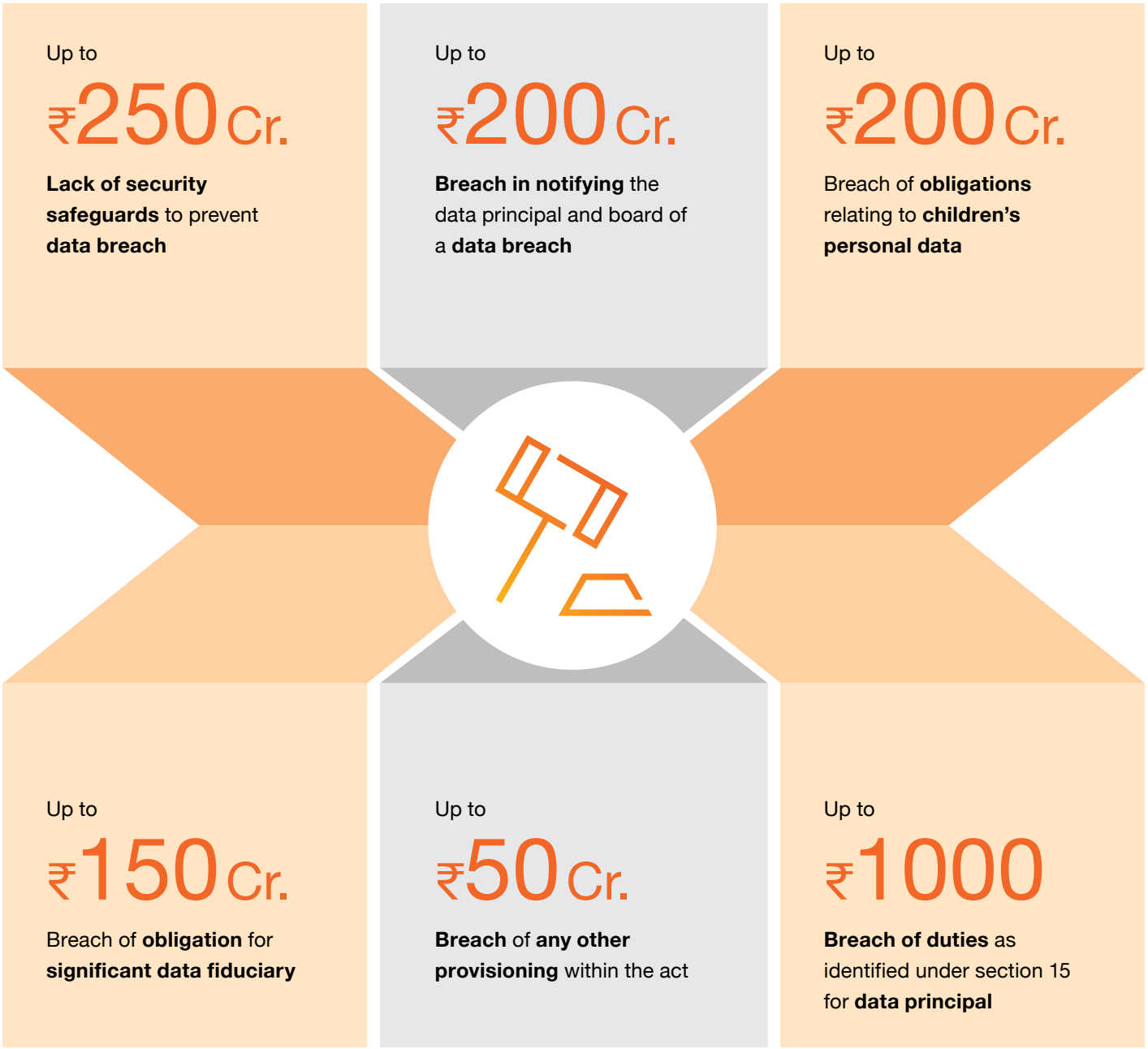
Consumers that are aware of privacy laws are likely to be receptive to AI, while those who are not may become alienated or migrate to other providers. While financial institutions across the globe are reluctantly searching for investment opportunities in the AI space, the governance, data privacy, and regulatory transparency around such adoption is critical in determining its viability and gaining customer trust.

For India's BFSI and FinTech industries, the confluence of the DPDPA and AI represents opportunity and threat—making it imperative for firms to future-proof their strategies. Entities that can demonstrate responsible and ethical use of data in AI applications would exhibit greater chances of gaining the privacy edge.

07

The regulatory stick: Penalties and non-compliance

Figure 3: Data breach penalties and related fines in India



Source: DPDP Act, 2023

08

Sectoral implications of data privacy

8.1 BFSI sector

8.1.1 Banks, NBFCs, and payment systems

Banks and large NBFCs have already been subjected to the Reserve Bank of India (RBI)'s cybersecurity guidelines, IT outsourcing norms, and data localisation expectations and are now facing the DPDPA as another layer of horizontal governance. As likely significant data fiduciaries (SDFs), bank and NBFC payment system providers must conduct data protection impact assessments (DPIAs) for data processing, appoint data protection officers (DPOs), and retain audit trails for compliance. In this context, the implications for the banking sector emerge in three primary areas:

- **The trust anchor:** With their likely status as SDFs, banks and other financial institutions are witnessing a paradigm shift in their privacy approaches from just ticking checkboxes to becoming an auditable function, driven by DPOs and governed through DPIAs.
- **The dividing line for payments:** UPI and payment applications' privacy is likely to function as a force that unbundles and distinguishes between core payment data and information that may be used for ancillary purposes such as analytics and marketing for monetisation, requiring specific user consent.
- **The balancing act:** Amidst the drive to limit and restrict the private data they hold, process, and analyse, banks must walk a tightrope between reducing the informational attack surface and retaining enough information for model improvement to effectively defend against fraud.

8.1.2 FinTech lenders, BNPL, and embedded finance

To make lending and payment collection decisions, digital lenders, buy now pay later platforms, and embedded finance providers are highly reliant on data such as device, application, transactional, and social connection data.

The DPDPA challenges this status quo in three ways:

- **Justify data use:** These organisations must clearly explain why users are being profiled, particularly in cases when the user data is indirectly sourced or inferred.
- **Be transparent:** They must clearly inform borrowers how exactly their data influences credit decisions or loan-related outcomes.
- **Stop data hoarding:** They must respect rules pertaining to purging or retention of these data, even if previous collection systems were designed to store data indefinitely.

While the RBI guidelines for digital lending comprehensively detailed fairness and transparency requirements, the DPDPA adds an additional layer of scrutiny, challenging businesses to rethink their processes around data-driven credit decisions, particularly in terms of indirect and aggregated data sources.

8.1.3 Wealth, insurance, and regulatory technology

Wealth management platforms and digital brokers gather data pertaining to users' preferences, risk appetites, and trading behaviours to identify preferences and sell more targeted products. In a similar fashion, insurers analyse users' PHI and lifestyle details to quantify premiums, while insurers mine extensive datasets to comply with KYC and anti-money laundering obligations.

The DPDPA introduces three critical changes to all these areas:

- **Separating 'need' from 'good-to-have':** Companies must clearly segregate what is mandatorily required and what is also required for personalisation or sales-related pitches.
- **Locking down sensitive data:** Breach of any PHI, biometrics details, or financial information can incur huge fines and penalties; therefore, these firms must use extremely stringent security measures for sensitive data types.
- **Taming AI risk:** As AI is increasingly being used in decision-making in areas such as lending or insurance, the law requires that these systems be designed in a way that their decisions can be justified and shown to be non-discriminatory.

8.1.4 Data processors, BPOs, and technology vendors

BPOs, IT service providers, and technology vendors that process data on behalf of BFSI clients must update contracts, security measures, and breach response procedures to reflect the DPDPA's core fundamental requirements. Although the onus of compliance is primarily the responsibility of data fiduciaries, processors that do not implement adequate safeguards risk financial and reputational repercussions.

The sector is likely to witness two primary effects:

- Standard DPDPA-related clauses in master services agreements
- Increased demand for independent audits, certifications, and attestations primarily focusing on DPDPA readiness

8.1 Healthcare and healthtech

Overview

This sector consists of traditional healthcare providers such as hospitals, clinics, labs, and pharma, as well as modern digital health players, such as telemedicine platforms, health apps, wearables, remote monitoring, and AI diagnostics.

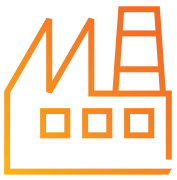
Data involved

Data include patients' medical history, diagnostic results, patient records, treatment plans, prescription details, insurance, health claim details, and identifying information linked to health services.

Privacy impact

- Secondary use and re-identification risk: Many clinical and behavioural datasets derived from research or AI training algorithms may be vulnerable to patient re-identification if combined with other data.
- Blurred lines between health and non-health data: Consumer apps, location data, and search histories can reveal health insights, even outside regulated healthcare settings.

8.2 Manufacturing and Industry 4.0



Overview

This sector includes interconnected supply chains, industrial IoT environments, and smart factories where daily operations such as production, maintenance, and logistics are driven by sensors, robotics, and other digital capabilities.

Data involved

Data include biometric access logs, wearable sensor data, employee records, vendor-related data, operational telemetry, production logs, supply chain information, and maintenance records linked to the workforce and plant operations.

Privacy impact

- Cross-border data flow: Global supply chains and cloud-based enterprise resource planning data are at risk of being scrutinised by multiple privacy regimes and restricted data transfers.
- Convergence of OT and IT: OT and IT convergence expands the potential attack surface and further complicates data classification and access controls.

8.3 E-commerce and retail

Overview

E-commerce platforms and omnichannel retailers collect extensive personal data, spanning browsing histories, loyalty programmes, transaction records, payments, and advertising data.

Data involved

Data include browsing histories, transactions, loyalty programmes, payment details, and targeted advertising ecosystems.

Privacy impact

- Increased privacy exposure occurs across profiling, cross-border data transfers, trust-sensitive customer interactions, and third-party data sharing.

8.4 Telecom and 5G ecosystems

Overview

Telecom operators stand at the junction of connectivity, identity, and geographical data acting as infrastructure providers for consumers, enterprises, and large-scale IoT ecosystems deployed over the 5G network.

Data involved

Data are related to SIM information, location-linked data, KYC records, call records, data session logs, identity verification data, messaging metadata, and OTP-linked service data.

Privacy impact

- Location and signalling data: 5G networks enable enhanced geolocation capabilities, which can yield highly sensitive individual-level insights when combined with other data sources.
- IoT and massive machine-type communications: Millions of connected devices generate huge amounts of behavioural data, with unclear consent.

8.5 Automotive and connected mobility

Overview

This sector covers smart mobility products such as connected cars, autonomous vehicles, and electronic vehicles, along with mobility service providers (car sharing, ride hailing), telematics, and insurers.

Data involved

Data include vehicle telemetry, in-vehicle sensor, and camera data; location, driver behaviour, and biometric data; user account and payment details; and service, insurance, and mobility platform-linked data.

Privacy impact and challenges

- In vehicle monitoring: Connected cars typically have multiple sensors and cameras that can capture drivers' and passengers' biometric and behavioural data, raising questions about privacy.
- Data sharing across ecosystems: Original equipment manufacturers, suppliers, mobility platforms, and connected car providers must define clear roles and responsibilities and implement standardised technical and organisational controls.

09

Tech privacy map

Different technologies have different privacy risk levels based on factors such as data sensitivity, volume, and regulatory scope. The heatmap below illustrates how data sensitivity, data volume, and regulatory influence shape the impact of privacy requirements across different technologies, helping prioritise controls when required.

Technology	Data sensitivity	Volume of data	Regulation influence	Overall privacy impact
FinTech				
AI				
Biometrics				
Cloud computing				
Blockchain				
IoT				
5G network				

Legend

Very high	
High	
Moderate	
Low	

10

Privacy as a business enabler: Creating a culture of trust

10.1 Trust as a new growth currency

Businesses grow when their customers feel safe and trusted, and privacy has become a key element in building this sense of security. It has become essential to not only protect data but also gain and maintain customers' trust and confidence. In other words, privacy has become a marketing tool that can help shape customers' decision-making and promote business growth.

According to a PwC survey, 93% of business executives agree that building and maintaining trust improves the business profitability.[21] It can thus be inferred that customers are less willing to support a business if they do not feel safe and secure. It also validates the argument that if businesses fail to maintain customer trust, they will lose on the bottom line.

10.2 Privacy as a marketing differentiator

In the world of marketing, privacy-oriented strategies are an exceptional game changer and differentiator. A Harvard study demonstrated that being transparent with customers concerning personal data use increases advertising click-through rates by 11% and revenue by up to 38%. Brands that adopt ethical and transparent data protection practices are more likely to gain consumers and make privacy a unique selling proposition.[22]

For instance, large technology companies have leveraged and benefited from privacy as a unique selling proposition for their product.

10.3 Privacy-led product innovation

Data privacy requirements compel businesses to rethink and innovate by integrating privacy concerns into product design. Organisations are focusing more on 'privacy by design' features, such as on-device processing and differential privacy, to deliver customised and tailored experiences to customers without compromising on data.

10.4 Privacy–profit equation

A Cisco report revealed that businesses can expect to gain a return of $2.70 for every dollar invested in data privacy. This is strong evidence that privacy isn't a cost centre but a profit driver.[23]

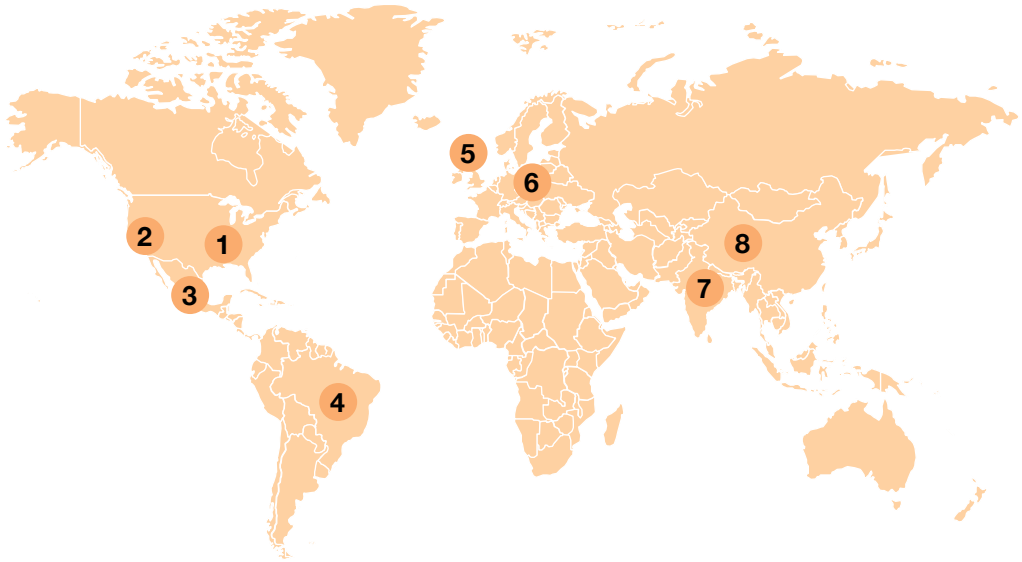
21 https://www.pwc.com/us/en/library/trust-in-business-survey.html
22 https://www.forbes.com/councils/forbestechcouncil/2022/09/23/exploring-privacy-as-a-competitive-advantage/
23 https://www.forbes.com/councils/forbestechcouncil/2022/09/23/exploring-privacy-as-a-competitive-advantage/

11

The global privacy landscape

Countries across the globe have recognised the need for robust privacy laws to protect personal data and strengthen individual rights. Consequently, jurisdictions have introduced diverse regulatory frameworks: the EU enforces GDPR, India follows the DPDPA, the US applies sector-specific laws, while China, Brazil, the UK, and others implement comprehensive privacy regimes.

Figure 4: The global privacy law landscape



1 Health Insurance Portability and Accountability Act (HIPAA)

Mandates a myriad of privacy, security, and breach notification requirements regarding protected health information (PHI)

2 California Consumer Privacy Act (CCPA)

Designates an array of new rights regarding California residents' personal data, starting with the right to be informed about what kinds of personal data companies have collected

California Privacy Rights Act (CPRA)

Expands rights designated in the CCPA and designates additional rights regarding California residents' personal data, including removing employee exemption and creating the California Privacy Protection Agency

3 Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Applies to private individuals or legal entities that process personal data for commercial use

4 Brazil's Lei Geral de Proteção de Dados (LGPD)

Uses Europe's GDPR as the blueprint for a national privacy framework for Brazil

5 UK Data Protection Act

Aims to modernise data protection laws to ensure they are effective in future

6 General Data Protection Regulation (GDPR)

Gives regulators unprecedented power to impose fines for privacy violations, requiring wide-scale privacy changes across organisations operating in the EU

7 India's DPDP Act, 2023

Passed in August 2023, the DPDP Act is a framework that defines individuals' rights to protect their personal data and the processing of the same for lawful purposes

8 China's Cybersecurity Law

Establishes new requirements for user consent in China, as well as for personal data collection, storage, and sharing

12 Conclusion

India is rapidly evolving from an agriculture-based economy to a digital and a data-driven economy which is fuelled by India's UPI payment systems, digital public infrastructure, and rapidly proliferating AI, which has made data privacy not just an individual concern but a systemic risk. The DPDPA provides a foundational process, technology, and legal architecture to manage these concerns, with serious implications for financial institutions and FinTech companies that are at the centre of everyday data flow.

A major concern for BFSI companies and FinTech leaders is not just treating the DPDPA as a data protection checklist but considering it as an opportunity for redesigning and reinventing data practices built around accountability, trust, and resilience. Organisations that incorporate privacy into their technology stack, customer experiences, and AI governance will be better positioned to thrive in India's new data economy and potentially influence global standards in the process.

Notes

Notes

About Unified Fintech Forum (UFF)

The Unified Fintech Forum (UFF), formerly known as the Digital Lenders Association of India (DLAI), stands as a pivotal non-profit Fintech sector Industry Association at the forefront of India's dynamic financial technology landscape. Established in October 2016 as a Section 8 company (not-for-profit) registered with the Ministry of Corporate Affairs, UFF has evolved significantly to represent the broader FinTech ecosystem. This mission and vision of UFF reflects the organization's commitment to fostering collaboration, innovation, and responsible growth across diverse FinTech domains, including payments, wealth tech, InsurTech and embedded finance. UFF currently has 190+ members engaged in digital financial services and fintech.

UFF serves as a unified voice for myriad FinTech companies operating in India, playing a crucial role in shaping the regulatory environment, promoting best practices, and driving financial inclusion nationwide. Its current diverse membership base, exceeding 120 entities, encompasses regulated lenders (NBFCs, Banks), FinTech platforms, embedded finance players, technology providers, credit bureaus, legal firms, and industry advisors. This wide representation allows UFF to address the evolving needs of the sector comprehensively.

A core pillar of UFF's mission is client protection. Recognizing the accelerated adoption of FinTech services, UFF has proactively championed initiatives to safeguard consumer rights and interests, particularly for those accessing digital credit and other digital financial services. It was among the first industry bodies to introduce a Voluntary Code of Conduct for digital lenders, outlining clear principles on transparency, responsible lending, fair collection practices, grievance redressal, and data privacy. This code has served as a benchmark for ethical practices and has significantly informed regulatory policy, including the Reserve Bank of India's (RBI) digital lending guidelines. UFF also actively collaborates with consumer rights organizations and legal experts to address emerging risks like predatory lending and digital fraud, reinforcing trust and accountability in the FinTech space.

Beyond advocacy and client protection, UFF is deeply engaged in capacity building within the Indian FinTech ecosystem. It recognizes the rapidly evolving regulatory, technological, and business landscape and strives to equip stakeholders with the necessary knowledge and skills. UFF regularly conducts workshops, masterclasses, and webinars on critical topics such as regulatory compliance, data privacy, fraud prevention, and inclusive product design. These initiatives are tailored for FinTech founders, compliance professionals, product managers, and technologists. By developing toolkits, explainer notes, and checklists in collaboration with policy experts and regulators, UFF simplifies complex regulatory frameworks and operationalizes compliance, fostering a culture of continuous learning and responsible growth. UFF is committed to advancing best practices, maintaining regulatory adherence, and supporting innovation to further financial inclusion in India. The forum's work is instrumental in ensuring that India's FinTech revolution remains inclusive, sustainable, and globally influential.

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Amol Bhat
Partner, Leader – Cyber and
Digital Risk, Financial Services
PwC India
amol.bhat@pwc.com

S Dinesh
Partner – Cyber and
Digital Risk, Financial Services
PwC India
s.dinesh@pwc.com

Shah Amber
Executive Director – Cyber and
Digital Risk, Financial Services
PwC India
shah.amber@pwc.com

Contributor

Mukul Kumar

pwc.in

HS/August 2026 - M&C 54335