



protiviti®  
Global Business Consulting

# NAVIGATING DPDPA IN BANKING

Compliance, Impact, and  
AI-Powered Strategies  
for Futureproofing







# CONTENTS

Foreword	05
Introduction and Background	07
The Banking Lens: Why DPDPA Matters	10
Compliance Foundations	13
Leveraging Technology for DPDPA Compliance	22
Futureproofing Privacy Programs	23
Conclusion and Roadmap	26
About IBA	30
About Protiviti	30
Our Recent Reports	31







**Sandeep Gupta**  
Managing Director  
Protiviti Member Firm for India

# FOREWORD

---

As the digital economy continues to evolve, data has become both a strategic asset and a regulatory obligation. The introduction of the Digital Personal Data Protection Act (DPDPA), 2023, along with the draft DPDP Rules, 2025, signals a pivotal transformation in India's data governance landscape—especially for the banking sector, which lies at the intersection of trust, technological innovation, and regulatory scrutiny.

Today's banks serve not only as guardians of extensive personal and financial data, they are also at the forefront of adopting emerging technologies like Artificial Intelligence (AI) to improve customer experiences, streamline decision-making, and strengthen fraud detection. While these advancements unlock significant value, they also bring forth new challenges related to privacy, algorithmic transparency, and data ethics. The DPDPA mandates a fundamental shift in how banks manage data—requiring them to balance innovation with the imperative to uphold individual rights and safeguard personal information.

In this context, customer trust becomes the cornerstone of sustainable digital transformation. As data privacy expectations rise, banks must demonstrate transparency, fairness, and accountability in every interaction. A robust privacy framework is no longer just a compliance requirement—it is a key driver of customer loyalty and institutional credibility.

This thought leadership aims to guide banking executives, data privacy and compliance officers, and technology strategists through the shifting regulatory landscape shaped by the Digital Personal Data Protection Act (DPDPA). With a focus on the banking sector, it examines how the DPDPA intersects with existing frameworks from regulators such as the RBI and SEBI. The document offers practical strategies for achieving compliance, reducing regulatory risk, and building resilient systems that are equipped to handle future changes.

At Protiviti, we believe that privacy and innovation are not mutually exclusive—they must go hand in hand. By integrating privacy by design, adopting privacy-enhancing technologies, and aligning AI governance with evolving regulatory standards, banks can create robust, customer-focused data ecosystems. This paper represents a step towards that vision, where compliance drives trust, and responsible data stewardship becomes a strategic differentiator for banks.

We sincerely thank the Indian Banks' Association (IBA) for their invaluable partnership in this initiative. Their support has been crucial in capturing insights from across the banking sector, helping ensure this report reflects the diverse realities of Indian financial institutions. Together, we remain committed to building a strong and secure digital ecosystem in India—where data privacy is embraced not only as a regulatory obligation but as a strategic priority.





# 1

## Introduction and Background

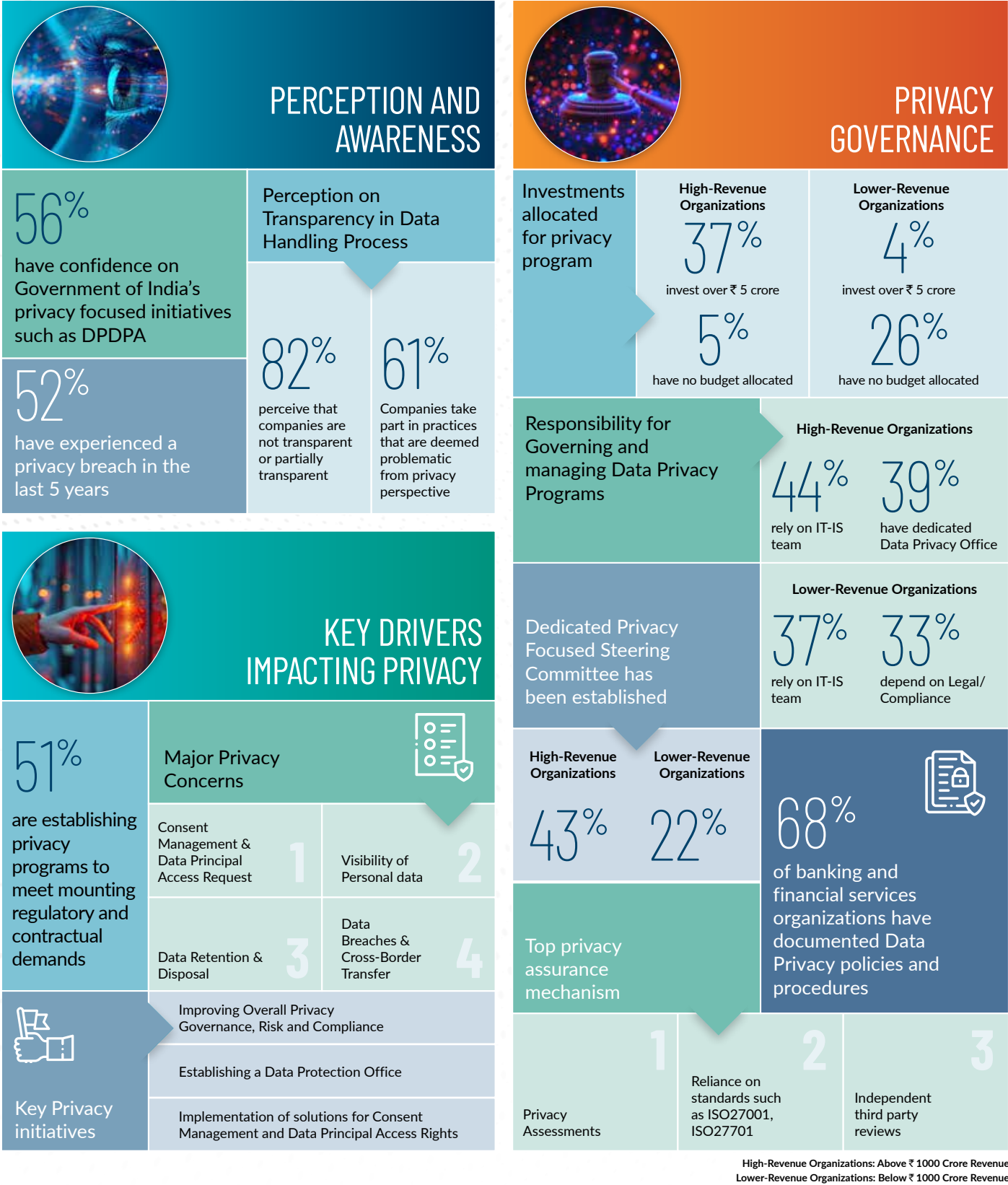
As the data protection regulations have become a global priority, India's regulatory environment also achieved an important milestone by enacting Digital Personal Data Protection Act (DPDPA), 2023 and releasing of the draft DPDP Rules, 2025 to safeguard individual's personal data and privacy rights.

As we move forward, enforcement and compliance with the new data protection regulations will have an enormous impact, particularly on banks who are the custodian of huge volume of financial and personal data. For banks, complying with DPDPA will not be a matter of legal compliance but will be an existential imperative in an environment where privacy needs to be a core part of the business and operational processes.

At Protiviti, leveraging our expertise in privacy and data protection, we delve into the implications of DPDPA for banks, decoding its intersection with sectoral regulations provided by RBI and SEBI, the operational and technological shifts required, and how institutions can futureproof their data privacy strategy to ensure compliance, resilience, and trust in the digital age.



Drawing from the State of Data Privacy in India – Survey Report, where the banking sector emerged as the most represented industry, the following insights highlight key readiness gaps and challenges—establishing a baseline as we explore the path forward.








## PRIVACY PROGRAM MATURITY

Organizational Maturity in Privacy Programs			Data Retention and Disposal Processes	Privacy Risk from Third Parties	Preparedness or Incident Response
26%	42%	32%	48%	38%	44%
privacy program is implemented	privacy program is defined	privacy program is not established or in planning stage	have their data retention & disposal process fully defined and implemented	address privacy concerns with third parties through both contractual agreements and risk assessments	remain at lower maturity levels, with non-proactive approaches for incident response processes
Privacy Focused Skilled Resources			Managing cross border transfer		Readiness for Managing Privacy in Emerging Technologies
	High-Revenue Organizations	Lower-Revenue Organizations			
In house privacy skill	58%	30%			
Support from third party organization	36%	41%	62%	20%	24%
Resourcing not planned	6%	29%	Through data localization and legal agreements	Yet to define appropriate measures	feel prepared to manage privacy concerns associated with Emerging Technologies



## EMBRACING TECHNOLOGY

 <b>Top Automation Initiatives in Privacy</b>	Privacy Rights and Consent Management		 <b>Enhancing Privacy Through Digital Identity</b>	39%	27%	22%
	PIA/DPIA/TPRM			Manage privilege access via PAM	utilize PAM for privilege users & enterprise IAM for managing end users	Not planned or in planning stages
	Data Governance (Data discovery / inventory)					

High-Revenue Organizations: Above ₹ 1000 Crore Revenue  
Lower-Revenue Organizations: Below ₹ 1000 Crore Revenue



# 2

## The Banking Lens

# Why DPDPA Matters

In the banking sector, where data forms the backbone of operations, customer trust is paramount. Banks are entrusted with personal data, financial records, identity documents, transaction data, biometric and geo location data making them prime targets for cyber-attacks and data breaches ultimately transforming data protection from a mere regulatory requirement into a strategic priority to gain customer trust.

While strategic prioritization is important for bank's reputation, the regulatory dimension cannot be ignored. The DPDPA sets forth key obligations that will affect the operational process of banks related to collection, storage, processing, transfer, deletion and disposal of personal data. Non-compliance with the DPDPA would lead to severe penalties which can hinder the bank's reputation and its financial standing.

As banks redefine their data operating procedures under the DPDPA, it will be interesting to see how this new act will complement and converge with the current sectorial guidelines and regulatory standards including the Reserve Bank of India (RBI) guidelines and Securities and Exchange Board of India (SEBI) regulation. The integration of the DPDPA into the existing sectoral regulatory landscape will create both opportunities and challenges. Banking sector will require a cohesive data governance and privacy strategy, that integrates a framework for innovation within the boundaries of data privacy and security.

Let's first look at the some of the privacy risks unique to the banking sector that pose as a privacy compliance challenge.



# Unique Privacy Risks in the Banking Sector

CATEGORY	RISK	DESCRIPTION
<b>Consent, Purpose Limitation &amp; Lawful Use</b>	Improper consent collection	Failure to obtain valid, granular, and informed consent for each specific purpose of data processing.
	Purpose creep	Using collected data beyond the originally stated purpose (e.g., upselling insurance using KYC data).
	Insufficient parental consent	Inadequate mechanisms for obtaining verifiable consent for processing children's data (under 18).
	Use of data beyond original purpose	Using personal data for fraud analysis, risk profiling, or customization without explicit consent may contravene DPDPA's purpose limitation and lawful processing clauses.
<b>Governance, Accountability &amp; SDF Obligations</b>	Lack of governance frameworks	Absence of well-defined data protection policies, roles (e.g., DPO), and regular reviews.
	Non-compliance with Data Principal rights	Delayed or incomplete response to access, correction, erasure, or grievance redressal requests.
	Failure in privacy by design	Systems and services not incorporating privacy controls during development or integration.
<b>Third-Party &amp; Vendor Risk</b>	Lack of processor oversight	Inadequate contracts and monitoring for vendors processing personal data on behalf of banks.
	Cross-border data transfer without safeguards	Sending personal data outside India without ensuring DPDPA-compliant protections.
	Aggregation risks via FinTech APIs	Risk of uncontrolled data sharing via third-party integrations (e.g., loan marketplaces, NBFC apps).
	Excessive reliance on external processors	Interaction with multiple third-party processors increases exposure to privacy risks, despite contractual safeguards. Ultimate responsibility still lies with the bank.
<b>Cybersecurity &amp; Breach Notification</b>	Unauthorized access or breaches	Data exposure due to weak internal controls or cyberattacks.
	Lack of breach notification readiness	Delays in notifying the Data Protection Board and affected individuals within required timelines.
	Over-retention of data	Retaining personal data beyond business or legal necessity, increasing breach exposure.
<b>Governance, Accountability &amp; SDF Obligations</b>	Stricter compliance obligations	Banks are likely to be classified as SDFs due to large data volume and sensitivity.
	Failure to conduct DPIAs	Missing mandated Data Protection Impact Assessments for high-risk processing (e.g., profiling, biometrics).
	Inadequate DPO oversight	Appointing a DPO in name only, without clear responsibilities or escalation frameworks.
<b>Automation, AI/ML &amp; Profiling Risk</b>	Automated decision-making without explanation	Use of credit scoring or fraud detection tools without transparency or recourse to Data Principals.
	Profiling without safeguards	Behavioral profiling (e.g., spending habits) without applying fairness, accuracy, and bias controls.
<b>Operational Compliance</b>	Inadequate documentation of processing	Missing data flow maps, ROPA (Record of Processing Activities), and audit trails.
	Insufficient training and awareness	Employees unaware of DPDPA compliance requirements and data handling responsibilities.
<b>Data Quality, Integrity &amp; Exploitation</b>	Erroneous data processing and classification	Sharing large datasets between systems may lead to miscomputed credit scores or incorrect KYC classification, resulting in financial exclusion or reputational loss.
<b>Technology Infrastructure Risk</b>	Outdated data architectures and lack of privacy-by-design	Legacy systems lacking modern privacy controls increase the risk of unauthorized access or data leakage due to insecure data handling practices.

The banking sector has distinct data risks that distinguish it from other sectors. Banks not only deal with huge volumes of personal and fiscal data but also processes high volume real-time transactions (eg. Online banking, payments, credit check, instant fund transfer etc.)

Together, these privacy risks highlight the urgent need for banks to design a strong data privacy framework that integrates

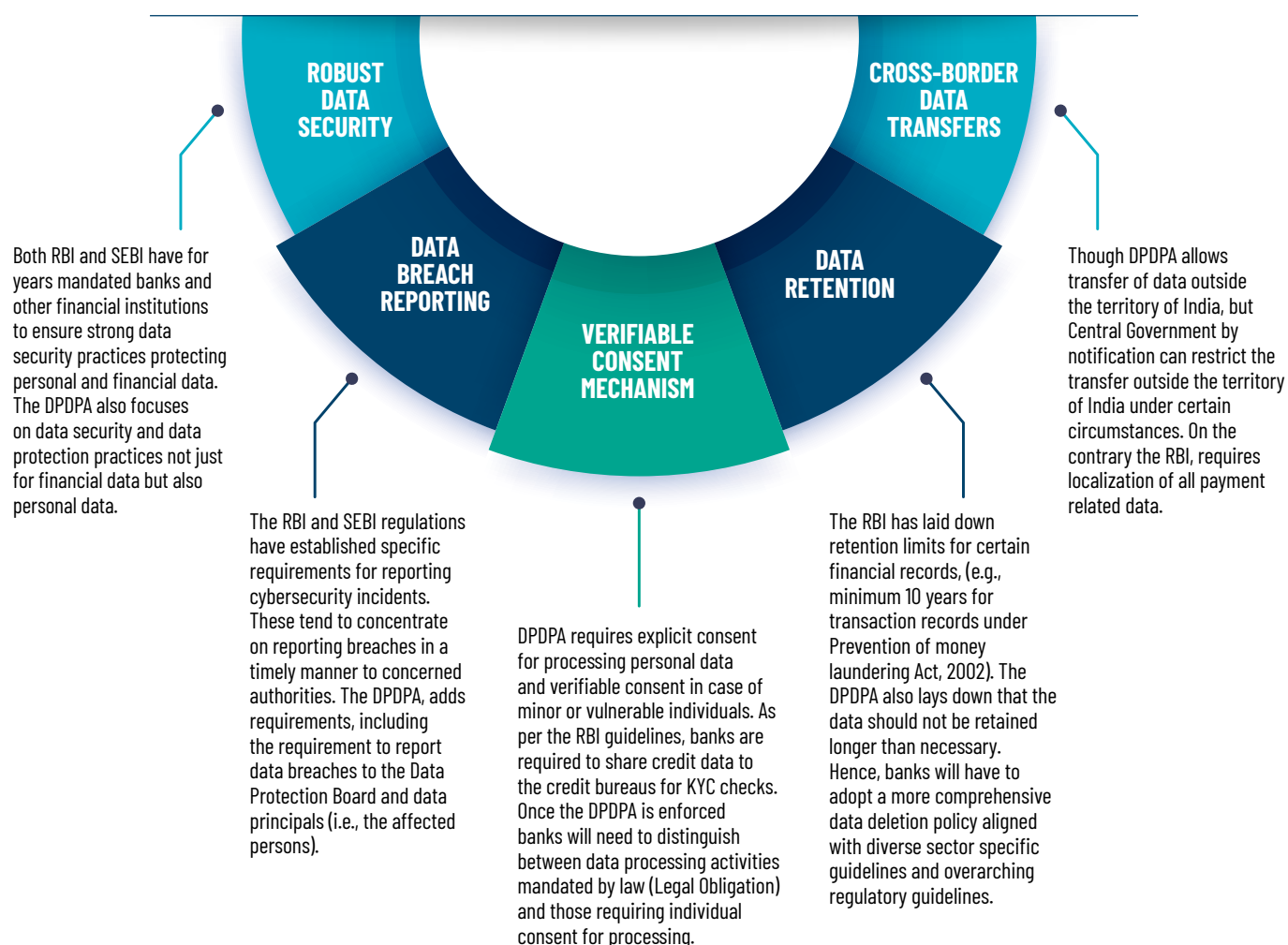
with the three key pillars of an organization i.e. people, processes, and technology. The framework needs to be holistic with unification of not just DPDPA principles but also the sectoral guidelines. To enable this, one needs to understand how the DPDPA overlaps with the current regulatory guidelines of RBI and SEBI.

# Regulatory Intersections: RBI, SEBI guidances and DPDPA/Draft DPDP rules

Banks in India are already subject to stringent regulations from the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI) which govern financial transactions, customer data, financial market practices etc. The DPDPA, while prioritizing data protection, interacts with these existing frameworks, giving rise to overlapping compliance requirements.

It has always been a priority for the **RBI** to protect customer data, particularly financial transaction data. With the

introduction of the DPDPA, banks must now balance these security measures with other data protection standards such as consent, data minimization, and privacy by design. The same applies to SEBI guidelines, which require customer data protection in the securities market. With the DPDPA providing new requirements, banks will have to incorporate these into their current processes, particularly in the case of investment-related data and trading processes.



For banks, these regulatory crossroads will mean having an overarching data privacy framework that aligns the DPDPA's requirements with the operational imperatives of RBI, and the SEBI.



# 3

## Compliance Foundations

Compliance with the DPDPA is based on fundamental privacy values, each intended to assure that personal data is processed with minimal exposure.

### Key DPDPA Requirements for Banks

As banks manage the complexities of merging multiple regulatory requirements, it is important to initially understand their responsibilities as a Data Fiduciary.



#### Data Breach

##### Notification to Data Principal

Banks, as Data Fiduciaries, are required to promptly inform affected Data Principals about a data breach. The notification must include:

- Description of the breach, its nature, extent, timing and location
- Safety measures that can be taken by Data Principals to mitigate the risk
- Contact information of a person who can respond to Data Principal

##### Reporting to Data Protection Board

In parallel, banks must also report the breach to the Data Protection Board within 72 hours of becoming aware. The report should include:

- Description of breach, nature, extent, timing, safety measures etc.
- Broad facts related to the events, circumstances, Measures implemented or proposed
- Findings regarding the person who caused the breach
- Report regarding the intimations given to affected Data Principals.



## Cross Border Data Transfer

- Transfer of data outside the territory of India is permitted (Ref. Rule 14 DPDPA).
- However, Central Government by notification can restrict the transfer outside the territory of India under certain circumstances.



## Privacy Notice & Consent

Provide a clear and concise notice to the Data Principals (Ref. Rule 3 DPDPA) -

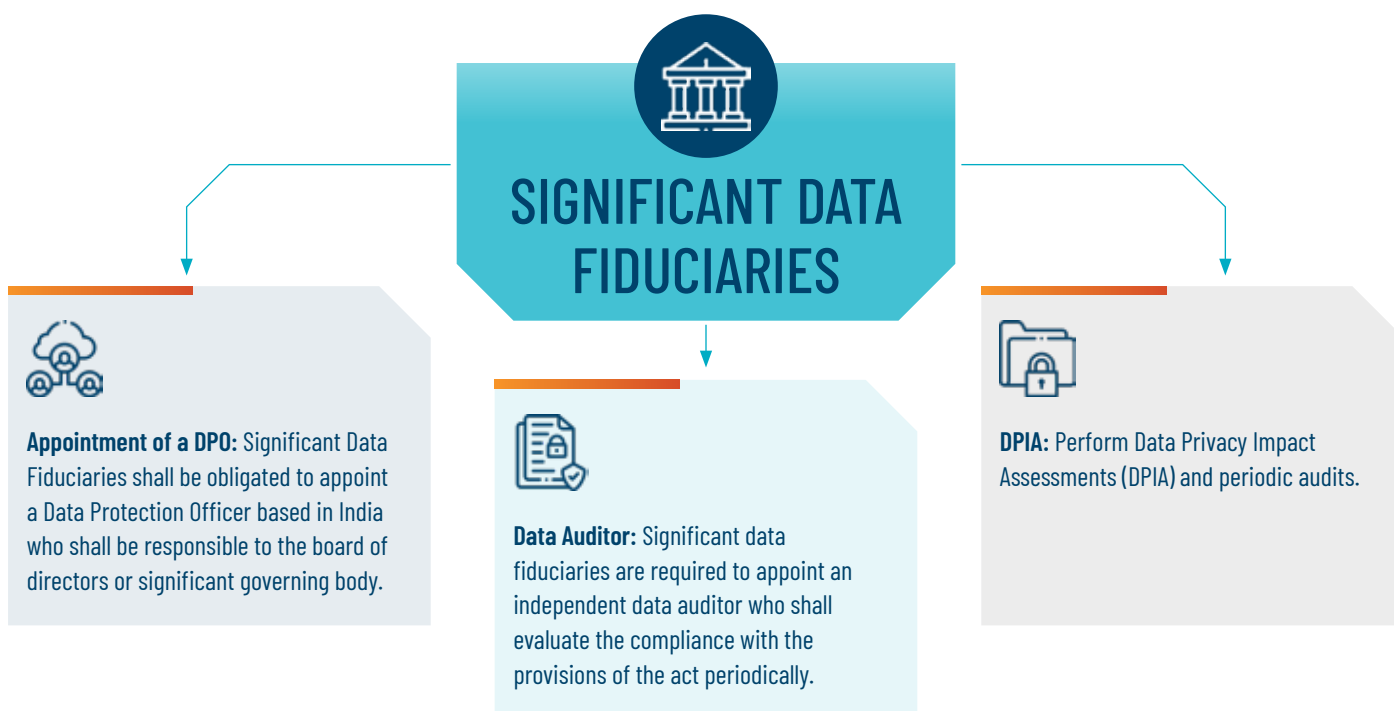
- Itemized list of personal data collected
- Purpose for processing of data
- Access to this information to be provided in English or any language specified in the eighth schedule of the Constitution of India
- Link to withdraw consent, exercise his/her rights and make compliant to the Board.



## Technical & Organizational Safeguards

- Protect personal data processed (Ref. Rule 6 DPDPA).
- Appropriate technical safeguards - encryption, obfuscation, masking, access controls, log monitoring etc.
- Appropriate organizational safeguards- policies, procedures, and contracts.

DPDP has also outlined supplementary obligations for organizations acting as Significant Data Fiduciaries. Though the classification criteria remain undefined, it is expected that we would get the clarity once the rules are finalized and Data Protection Board of India is established. As per the Act, probability of banks being classified as Significant Data Fiduciaries are higher due to the volume and the categories of personal data processed by banks. Hence, banks would be required to fulfil the following additional obligations once classified as SDFs:







The below tables outlines responsibilities for different categories of Data Fiduciary under DPDPA.

	Type of Data Fiducuries	Privacy Policy	Notice	Data Audits	Publishing in languages	DPIA	DPO	Data Erasure Request	Grievance Redressal	Correction or update request	Reasonable Security Procedures	Consent Managers
1	Significant Data Fiduciaries	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Data Fiduciaries	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓
3	Start-ups and other Similar data fiduciaries sec. 17(5)	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓

\*Banks would most probably be catagorized as Significant Data Fiduciary

# Roles of Data Processors, and Consent Managers

In the banking environment, personal data is processed on a diverse network of core banking solutions, fintech collaborations, outsourced partners, and digital service providers. Therefore, it is of utmost importance for banks to define and manage the roles of every entity involved in processing of personal data

**Outsourced Partners & FinTechs firms as Data Processor:** Banks rely on outsourced vendors for specialized services for their digital banking platform, KYC verification, customer analytics and fraud detection, payment gateway processing, chatbot and call center support.

Under DPDPA, these entities are defined as Data Processor who are processing data on behalf of the data fiduciaries. Though, the ultimate responsibility for ensuring processors comply with privacy and security rests with the data fiduciary, but data processors must ensure that they are compliant with the applicable regulation. This accountability should be mandated through contractual agreements (such as Data Processing Agreements as part of Master Service Agreement), audits and continuous oversight of the processor's activities.

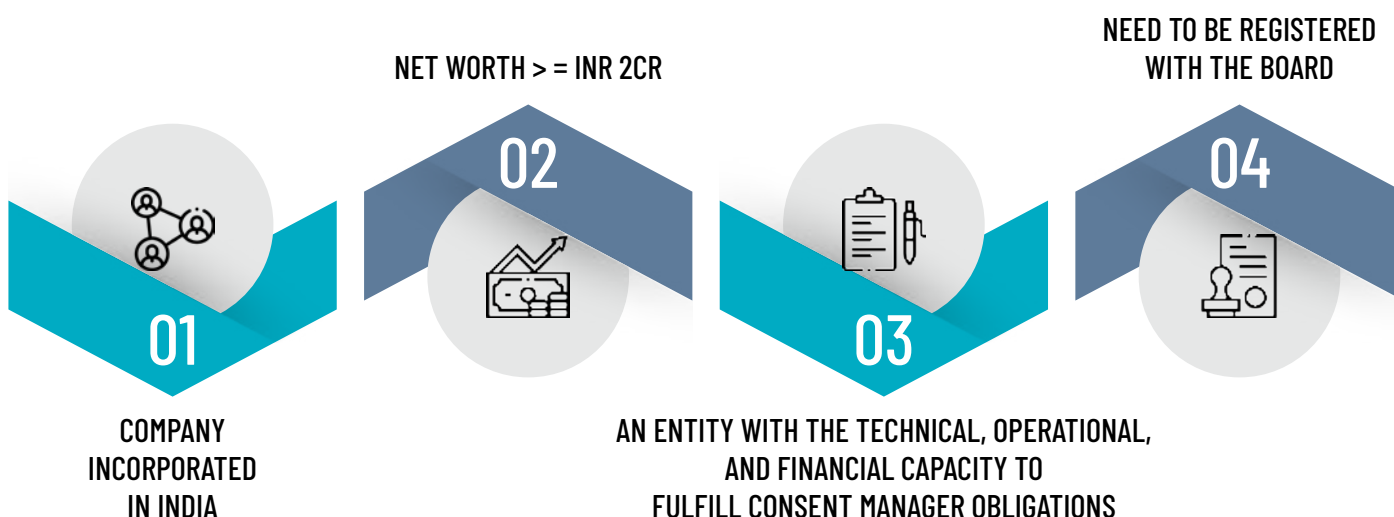
**Consent Managers:** A **Consent Manager** is a distinct role introduced under the DPDPA Act, designed to ease the complexities of consent management for both data fiduciaries and data principals. Consent managers would act as an independent entity, enabling data principals (banking customers) to provide, manage and withdraw their consent seamlessly across multiple fiduciaries through a unified interface.

Banks will be required to either:

- Integrate with external, registered Consent Managers, or
- Build internal capabilities that meet the DPDPA Act requirements

This operating model not only simplifies compliance for banks and their partners but enhances principal control over personal data making consent management more transparent & efficient. Yet, the true measure is how well these concepts and frameworks are executed in real world banking operations. From customer onboarding to third-party data sharing, there are many touchpoints for banks with which compliance and customer experience must harmonize.

## Who can be a Consent Manager





# DPDPA impact on critical banking functions

The DPDP Act has significant implications for critical banking functions, necessitating targeted compliance strategies and operational adjustments to ensure adherence. Below are the illustrative details of the same :

S. No.	Banking Function	DPDPA 2023 & DPDP Rules 2025 Compliance Requirements	Solutions for Compliance
1	<b>Customer Onboarding &amp; KYC</b>	<ul style="list-style-type: none"> <li>● Obtain explicit consent before collecting personal data.</li> <li>● Ensure purpose limitation (only for onboarding/KYC).</li> <li>● Implement strict data retention policies.</li> <li>● Restrict cross-border data transfers.</li> </ul>	<ul style="list-style-type: none"> <li>● Implement automated consent and privacy notices.</li> <li>● Use AI-driven identity verification.</li> <li>● Enforce data retention automation</li> </ul>
2	<b>Transaction Processing &amp; Payments</b>	<ul style="list-style-type: none"> <li>● Minimize data collection to necessary transaction details.</li> <li>● Encrypt all payment and transaction data.</li> <li>● Notify customers in case of breaches.</li> <li>● Ensure third-party payment processors comply with regulations.</li> </ul>	<ul style="list-style-type: none"> <li>● Use data masking &amp; tokenization technique for payment data.</li> <li>● Implement end-to-end encryption.</li> <li>● Establish breach monitoring and third-party compliance audits.</li> </ul>
3	<b>Loan &amp; Credit Processing</b>	<ul style="list-style-type: none"> <li>● Use personal data only for credit evaluation, not for marketing.</li> <li>● Provide customers with the right to correct their credit data.</li> <li>● Ensure AI-driven decisions are explainable and transparent.</li> </ul>	<ul style="list-style-type: none"> <li>● Deploy explainable AI models for fair credit decisions.</li> <li>● Provide self-service portals for data corrections.</li> <li>● Ensure compliance-driven data retention policies.</li> </ul>
4	<b>Customer Account Management</b>	<ul style="list-style-type: none"> <li>● Allow customers to access and correct personal data.</li> <li>● Provide clear privacy notices about data use.</li> <li>● Implement security controls for unauthorized access prevention.</li> </ul>	<ul style="list-style-type: none"> <li>● Develop self-service account update platforms.</li> <li>● Enforce multi-factor authentication (MFA). Leverage PIM/PAM solution</li> <li>● Provide privacy education to customers.</li> </ul>
5	<b>Fraud Detection &amp; Risk Monitoring</b>	<ul style="list-style-type: none"> <li>● Use privacy-preserving AI to detect fraud.</li> <li>● Ensure real-time monitoring of financial transactions.</li> <li>● Automate alerts for high-risk activities.</li> </ul>	<ul style="list-style-type: none"> <li>● Implement real-time fraud analytics with privacy safeguards.</li> <li>● Use AI for anomaly detection.</li> <li>● Conduct regular compliance checks.</li> </ul>
6	<b>Data Storage &amp; Retention</b>	<ul style="list-style-type: none"> <li>● Store only necessary data and avoid excessive retention.</li> <li>● Implement automated deletion of expired data.</li> <li>● Encrypt stored data to prevent unauthorized access.</li> </ul>	<ul style="list-style-type: none"> <li>● Automate data retention and deletion policies.</li> <li>● Implement encryption across cloud and on-premise storage.</li> <li>● Regularly audit stored data for compliance.</li> </ul>
7	<b>Data Sharing with Third Parties</b>	<ul style="list-style-type: none"> <li>● Obtain explicit consent before sharing data with third parties.</li> <li>● Ensure third-party vendors comply with DPDP rules.</li> <li>● Secure API integrations for safe data transfers.</li> </ul>	<ul style="list-style-type: none"> <li>● Develop secure API gateways for controlled access.</li> <li>● Enforce contractual agreements with data-sharing partners.</li> <li>● Maintain detailed audit logs.</li> </ul>
8	<b>Data Breach Handling &amp; Incident Response</b>	<ul style="list-style-type: none"> <li>● Implement real-time breach monitoring.</li> <li>● Notify regulators and affected customers promptly.</li> <li>● Have a structured incident response plan in place.</li> </ul>	<ul style="list-style-type: none"> <li>● Deploy advanced threat intelligence systems and SOC.</li> <li>● Automate customer notifications for breaches.</li> <li>● Conduct cybersecurity drills regularly.</li> </ul>

# Identifying personal data in a banking environment

A critical step for banks in aligning with DPDPA requirements is to map the lifecycle of personal data—specifically, where it is stored, processed, or transmitted. The following is an illustrative reference list to support this data flow identification effort

S. No.	IT Infrastructure Component	Function	Where Personal Data is Stored/Processed/ Transmitted?	Examples of Personal Data
1	Core Banking System (CBS)	The main system handling customer accounts, transactions, and banking services.	Stored & Processed in centralized databases and application layers.	Customer Name, Account Numbers, KYC details, Transaction History
2	Customer Relationship Management (CRM)	Manages customer interactions, complaints, and relationship management.	Stored & Processed in CRM databases.	Contact Information, Customer Preferences, Complaint History
3	Payment Processing Systems	Handles card payments, UPI, IMPS, RTGS, NEFT transactions.	Processed & Transmitted through encrypted payment gateways.	Card Details, Transaction Amounts, Beneficiary Details
4	Internet Banking & Mobile Banking Platforms	Provides online and mobile banking access to customers.	Processed & Transmitted over secure internet connections with encryption.	Login Credentials, Transaction Data, Device Information
5	ATM & POS Networks	Enables cash withdrawals, deposits, and in-store purchases.	Processed & Transmitted through banking networks.	Card Numbers, PINs, Transaction Details
6	Data Warehouses & Analytical Systems	Stores historical transaction and customer behavior data for analytics.	Stored & Processed for reporting and fraud detection.	Anonymized Customer Data, Financial Reports
7	Fraud Detection & Risk Management Systems	AI-based monitoring to detect suspicious activities.	Processed in real-time through AI models.	Transaction Patterns, Device Identifiers
8	Third-Party API Integrations (Open Banking, FinTechs, Credit Bureaus)	Allows external systems to access banking data.	Transmitted & Processed via secure APIs.	Credit Score Data, Account Balance, Loan Eligibility
9	Call Centers & Customer Support Systems	Handles customer queries and complaints.	Stored & Processed in secure call logs and CRM.	Customer Name, Contact Number, Call Recordings
10	Regulatory Reporting & Compliance Systems	Generates reports for regulatory compliance.	Stored & Processed in compliance databases.	Suspicious Transactions, KYC Compliance Data
11	Cloud & Data Storage Solutions	Stores backups, archives, and scalable banking data.	Stored in cloud/on-premise data centers.	Customer Profiles, Archived Transactions
12	Network & Cybersecurity Infrastructure	Firewalls, VPNs, and security monitoring to protect banking systems.	Transmitted over secure networks.	Encrypted Personal Data, Access Logs
13	Enterprise Resource Planning (ERP) Systems	Manages internal banking operations like HR, finance, and procurement.	Stored & Processed in ERP databases.	Employee Data, Payroll Records

# Case-Based Exploration of DPDPA in Banking Contexts

The **use cases** below showcase how the DPDPA will impact everyday banking operations



With the advent of digitization, banks use digital onboarding mechanisms to verify customer identity through Aadhaar, PAN, and biometric data. Customer Onboarding is one of the key functions of the bank in which a vast volume of personal data is collected and processed

Banks must now obtain:

- **Privacy Notice:** Notifying the data principals at the point of data collection- the purpose of collecting the personal data, categories of personal data collected, data transfer, how long data would be retained, exercising data principal rights etc.
- **Explicit Consent:** Banks must obtain explicit consent for collecting sensitive personal data. Ensure that requirements for managing consent for children (Below 18 years) are followed. Mechanism to opt-out, when relying on consent
- **Data Retention:** The personal data gathered at the time of onboarding should not be retained after the specified purpose is fulfilled. Consequently, banks need to formulate clear data retention policies and enforce secure deletion procedures to avoid regulatory sanctions.



Another key important obligation of the bank is to monitor customer transactions for patterns that indicate money laundering, such as unusually large or frequent transactions involving high-risk jurisdictions.

Though the transaction monitoring continues to be an essential requirement for the identification of suspicious behavior, how personal data is handled within AML procedures must conform to DPDPA's privacy-oriented paradigm. This adds a new type of compliance expectation that banks need to navigate with care in policy, operations, and global coordination.

- **Purpose Limitation:** Banks must make sure that data gathered for Anti-Money Laundering (AML) objectives is not used for irrelevant activities. This requires explicit policies that limit the use of such data exclusively to AML-specific activities, so there is less chance of unauthorized access or misuse.
- **Transparency:** The customers shall be made aware of AML related data processing activities, such as collection, use, and disclosure of their data.
- **Cross-Border Compliance:** AML activities relating to data sharing with global agencies should be in line with DPDPA and applicable sectoral regulations. . Banks must ensure that any data sharing across borders aligns with data protection laws, implementing appropriate safeguards like Standard Contractual Clauses (SCCs) and ensuring regulatory approvals are obtained.



### Use Case 3

## Risk Management

Banks perform periodic risk assessments to identify vulnerabilities in its operations, including cybersecurity threats, operational inefficiencies, and regulatory non-compliance. To manage risks effectively, the bank collects and processes extensive customer data, transactional records, and market analytics leading to a lot of data processing for its internal operations such as credit scoring, customer support and risk profiling. These processes must meet standards of necessity, proportionality, and fairness under the Act.

- **Enhanced Data Governance:** Ensuring that the personal data utilized for risk analysis is gathered and processed with express consent and in accordance with stated purposes for which it is being processed.
- **Auditability:** Keeping precise records of how the data is accessed, processed, and analyzed to maintain compliance.
- **Compliance Reporting:** Regular compliance reports will need to be submitted to the Data Protection Board of India.

### Use Case 4

## Investment Banking

Wealth management firms increasingly rely on AI-based analytics, market insight, and predictive modeling processing huge amounts of financial, demographic, and behavioral data to provide hyper-personalized portfolio suggestions. As banks grow more sophisticated in this area and extend their collaborations with third-party fintech and advisors, strong data protection and regulatory trust become core to the way these products are created, governed, and run.

- **Algorithmic Transparency and Fairness:** DPDPA mandates transparency in automated decision-making processes, ensuring fairness and non-discrimination in investment recommendations. Conducting Data Protection Impact Assessment (DPIA) before deploying AI driven systems and ensuring AI models are auditable would be important
- **Third Party Vendor Management:** Collaborating with third-party financial advisors and fintech partners to enhance investment strategies will necessitate strong vendor management controls via periodic third-party risk assessment, MSAs, DPAs outlining compliance expectations and data handling responsibilities.
- **Privacy by Design and Default:** Systems processing sensitive financial and behavioral data will need to be integrated with the core privacy principals at the design stage itself to ensure data is protected and compliant throughout the data lifecycle of the application.

## Use Case 5

# Exit Strategies and Mergers in Private Equity

Private equity (PE) firms frequently engage in exit strategies and mergers, which involve the transfer, consolidation, and restructuring of large volumes of financial, operational, and personal data of portfolio companies. These transactions require careful handling of sensitive personal data of employees, investors, and customers, making compliance with the DPDPA and other relevant regulations.

With high regulatory risk and personal data sensitivity involved, PE firms need to integrate privacy and security thinking into the transaction life cycle. This needs to be underpinned by a formalized approach to due diligence, risk management, and cross-border compliance, as shown below.

- **Due Diligence on Compliance:** As part of exit and merger processes, PE firms must assess the data protection compliance status of portfolio companies to identify potential regulatory risks by conducting Data Protection Impact Assessments (DPIA), including data protection clauses in the sale and merger agreements, identifying liabilities related to data breaches or non-compliance.
- **Cross-Border Data Transfer:** Exit and merger strategies involving international buyer and parent companies will require to assist the legal requirements of data transfers to foreign jurisdictions and receiving necessary approvals and keeping the regulatory authorities informed of cross-border data flow movements. Besides varying regulatory mechanisms will have to be converged.
- **Risk Assessment:** Cybersecurity risks should be carefully analyzed to make sure that the sensitive data processed in the transaction is appropriately protected. Cyber risks are heightened during mergers, with potential risks from system integration, unauthorized access, and insecure data transfers.

## Use Case 6

# Cross Selling by Insurance Providers

As Insurance providers engage in cross-selling of insurance policies, with DPDPA the cross-selling and packaged offering can only be initiated if the Data Principal has given his/her explicit consent. For data-driven cross-selling, therefore, the need now arises to shift from being convenience-driven to consent-driven, with transparency, purpose limitation, and legitimate data-sharing practices between partners and platforms.

- **Consent:** Consent will become crucial before insurers use existing customer data beyond its original purpose. Customers must opt-in for promotional activities, and should be provided with granular choices, such as consent for specific products (e.g., Health vs. Life Insurance) along with the option to opt out.
- **Third-Party Data Sharing Compliance:** Collaboration with third-party partners or brokers to offer bundled products, data-sharing agreements must ensure compliance with DPDPA. Contracts should clearly define data processing responsibilities and include safeguards for data protection.
- **Transparency and Privacy Notice:** Customers will need to be informed via comprehensive privacy notices that clearly outline how their data will be utilized to cross-sell, what type of data is being processed, and their rights (such as opting out of marketing messages). These notices must be made accessible throughout all touchpoints, keeping customers adequately informed prior to providing their personal data.



# 4

## Leveraging Technology for DPDPA Compliance

In the time of growing regulatory landscape, digitalization and automation, technology plays a key role in simplifying and streamlining compliance for organizations while achieving robust data protection. The below section delves into how leveraging modern privacy technology solutions can enable the organizations particularly banks into meeting regulatory requirements, reduce privacy risks and maintain data protection standards.

As banks seek to converge with the DPDPA, it is imperative that a combination of privacy platform and Privacy enhancing

Technologies (PETs) be considered to develop a privacy first solution across the banking ecosystem. Banks can leverage data privacy and protection tools available to ease their compliance efforts.

**(e.g.)** Implementing data discovery and classification tool to gain more visibility into personal data held in bank's disparate systems. In the same way, consent and data principal rights management platforms can assist in simplifying and automating the consent opt-in and opt-out and servicing of principal rights request for both the Data Principals and Data Fiduciaries.

In tandem with PETs, Privacy by Design also needs to be built in and integrated at the initial application/process development stage, ensuring application compliance throughout the data lifecycle (Collection, storage, processing, archiving and deletion).

**(e.g.)** Privacy notice at collection touch points, encrypting data while transferring, pseudonymizing and anonymizing wherever possible, integration with consent and data principal rights mechanisms, data deletion triggers post retention lapse.

If incorporated meticulously these Privacy-by-Design principles and technology enablers can be the building blocks for strong privacy risk management and business agility. At Protiviti, we collaborate with our clients to review these methodologies within the parameters of their operations so that they can balance operational feasibility with regulatory requirements.





# 5

## Futureproofing Privacy Programs

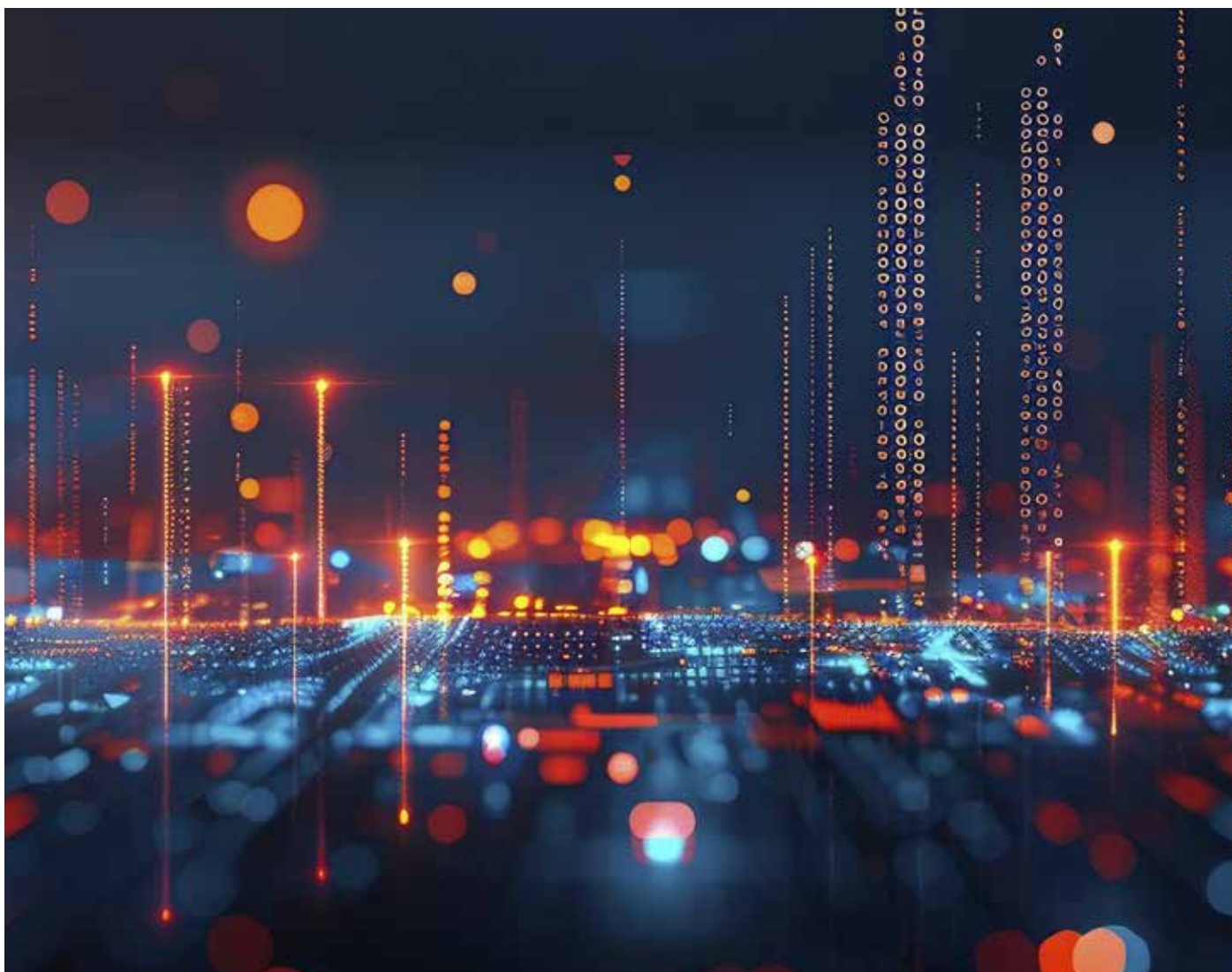
As banks align with the DPDPA, compliance must be treated as an ongoing commitment rather than a one-time exercise. With advancing threats, changing customer expectations, and regulatory amendments, futureproofing privacy programs by embedding privacy by design and default in processes, adaptive compliance frameworks and technology integration and automation is the key.

Sustainable privacy operations are the cornerstone of any data privacy strategy. For banks, this will involve taking risk-based approach, integrating privacy practices throughout the enterprise and strong governance.

- **Data Protection Office Establishment:** To instill privacy as an organizational strategic imperative, each bank should aim to establish a dedicated data protection office responsible

for privacy governance. This office should be led by a Data Protection Officer (DPO). This function need not just be focused on ensuring compliance with the DPDPA but serve as an operational center facilitating alignment between business, legal, technology, and risk functions from global privacy compliance standpoint.

- **Aligning Risk & Compliance:** For banks to have strong data protection controls, privacy needs to be fully embedded in their overall risk management system. This will allow privacy to be made part of the bank's overall risk approach, so that it is addressed along with other key compliance obligations. By integrating privacy with enterprise risk management, banks are able to recognize and address privacy-related risks in advance, providing ongoing compliance while upholding the trust of their customers.



➤ **Scalable technology and automation:** As banks adapt to growing data protection needs, the utilization of scalable tools and automation is necessary. Leveraging next-generation solutions like data discovery platforms, consent management systems, and rights fulfillment tools, banks will be able to seamlessly integrated privacy into their processes. These scalable technologies allow banks to manage increasing amounts of data efficiently while remaining compliant with changing regulations, in the end allowing the bank to better respond to new challenges around privacy.

➤ **Metrics & KPIs:** To effectively track the success and sustainability of their privacy programs, banks needs to have monitoring mechanism setup. Banks can track request fulfillment turnaround time, breach response readiness, cross border data transfers, business unit privacy maturity. The measurable insights into the efficacy of their current controls, non-compliant areas, areas of concern will help in providing better visibility

and transparency not only for early risk identification and mitigation but also for better governance and accountability.

➤ **Training and Governance:** A Data Privacy Operations program is only as good as the individuals who make and maintain it. As the regulatory environment evolves, continuous investment in governance, training and monitoring can help institutions remain prepared as well as embed privacy into the foundation of business operations. Organizations must emphasize delivering role-based training that reflect each role's unique set of privacy obligations, whether it is frontline customer service agents, IT staff, product developers, or senior management. This exercise will ensure that the people understand their privacy and regulatory obligation.

➤ **Conducting regular audits:** Periodic internal audits should be conducted to ensure that the privacy controls work effectively, assessing process gaps. External assessments can also assist banks in setting benchmarks against industry best practices and readiness for anticipated enforcement activities.

As regulatory expectations rise, harnessing AI to accelerate compliance and reinforce customer trust has become mission-critical. Below are some illustrative use cases demonstrating how AI is being applied in this context.

S. No.	Compliance Area	Generative AI Use Case	Description / Benefit
1.	<b>Consent Management</b>	Dynamic Consent Notice Generator	Auto-generate personalized, purpose-specific consent notices for various services (e.g., loans, KYC, app usage) in plain, regional language.
		Conversational Consent Assistant	AI chatbots that explain consent terms and obtain/verbalize digital consent in a traceable manner.
2.	<b>Privacy Notices / Policies</b>	AI-Generated Privacy Disclosures	Summarize privacy policies dynamically for different products, channels (web/app), and languages. Ensures updated and understandable information delivery.
3.	<b>Data Subject Rights (Access/Correction/Erasure)</b>	Auto-Response Engine for Data Principal Requests	Automate generation of responses to access, correction, or erasure requests using secure LLMs that reference internal records.
		Redaction Bots for Data Sharing	Redact non-requested or sensitive info from response documents to prevent over-disclosure when servicing DSARs.
4.	<b>Purpose Limitation Compliance</b>	Data Classification & Usage Summarizer	Use GenAI to summarize and label datasets to ensure alignment between data usage and collected purpose, helping detect misuse or purpose creep.
5.	<b>Record of Processing Activities (ROPA)</b>	ROPA Document Generator	Automatically generate and update Records of Processing Activities by parsing system logs and data flow diagrams.
6.	<b>DPIA (Data Protection Impact Assessments)</b>	Draft DPIA Reports Using AI	AI can generate initial drafts of DPIA reports, suggest impact ratings, and recommend mitigations based on previous assessments and input prompts.
7.	<b>Training &amp; Awareness</b>	Scenario-Based Compliance Training Simulators	GenAI can create realistic scenarios or roleplays for staff training on privacy obligations and breach handling.
8.	<b>Vendor / Third-Party Risk</b>	AI-Driven Privacy Clause Analyzer	Automate review and flagging of missing or non-compliant privacy clauses in vendor contracts.
9.	<b>Breach Notification</b>	Auto-Drafted Notification Letters	Draft breach notifications (to Data Protection Board or Data Principals) based on structured input (e.g., timeline, impact, remedial action).
10.	<b>Language &amp; Accessibility</b>	Multilingual Policy Translation	Translate privacy notices, consent forms, and rights explanation in vernacular languages using GenAI with privacy context.

The goal for the banks should be to shift from a reactive, siloed compliance model to a resilient, responsive privacy operating model. This operating model need not only adapts to changing regulations and market conditions but also future-proofs against technology changes to ensure banks have a resilient and proactive privacy model. To ensure the success of any key programs, the people are the most important, hence training them is of utmost importance.





# 6

## Conclusion and Roadmap





## Conclusion and Roadmap

The Digital Personal Data Protection Act (DPDPA) and the draft DPDP rules represents a critical change in the way that personal data needs to be managed, particularly in the banking industry where trust, security, and compliance converge. With banks processing huge amounts of sensitive information across ever-more sophisticated digital environments, DPDPA conformance is not merely a compliance requirement but a business imperative. The way forward is through integration of privacy by design in operations, the fortification of governance frameworks, and addressing risks on a proactive basis. Banks that treat compliance as an enduring capability instead of an upfront effort can both protect customer trust as well as derive value through responsible data stewardship.

At Protiviti, we understand these challenges and are committed to being your trusted partner in this journey. With deep expertise in data protection, privacy consulting, and regulatory compliance and sector specific SMEs we help organizations navigate complexities by assessing their current privacy state, designing and implementing robust frameworks, operationalizing compliance measures, and leveraging advanced privacy technologies. By taking a strategic and proactive approach today, businesses can not only ensure compliance with the DPDPA but also build a strong foundation for responsible data stewardship in an increasingly digital world—turning privacy into a competitive advantage rather than just a regulatory requirement.

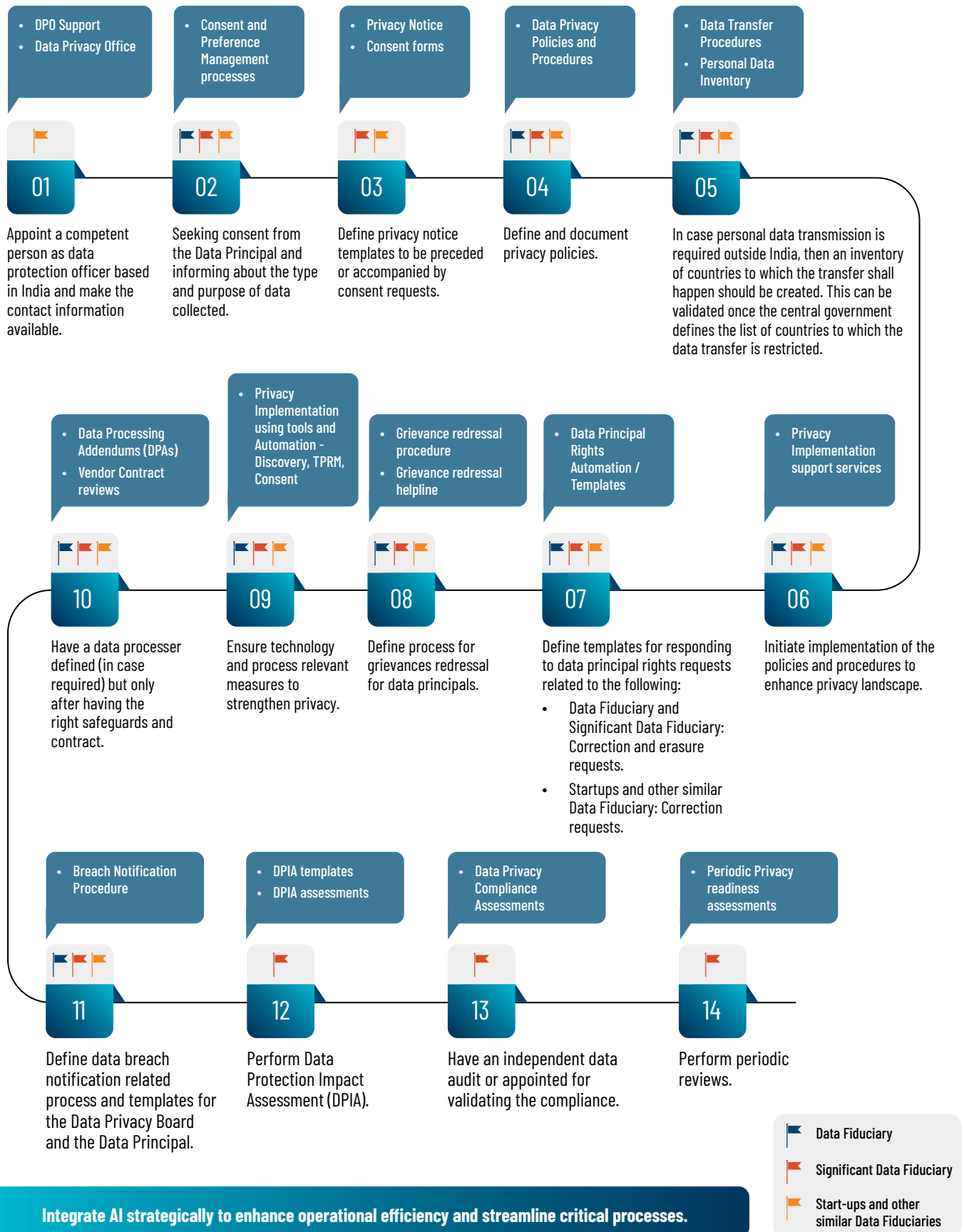




# KEY STEPS TO ATTAIN COMPLIANCE TO DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND DRAFT DPDP RULES, 2025



# Key steps to attain compliance to Digital Personal Data Protection Act, 2023 and Draft DPDP Rules, 2025



# About IBA

Indian Banks' Association (IBA), formed on (26 September 1946) as a representative body of management of banking in India operating in India - an association of Indian banks and financial institutions based in Mumbai. With an initial membership representing 22 banks in India in 1946, IBA currently represents 249 banking companies. IBA was formed for development, coordination and strengthening of Indian Banking, and assist the member banks in various ways including implementation of new systems and adoption of standards among the members.

## Address:

World Trade Centre Complex,  
6th Floor Centre 1 Building,  
World Trade Centre Complex, Cuff Parade,  
Mumbai – 400 005

**Tel:** 91-22-6923 4040 | 6951 5166

**Website:** [www.iba.org.in](http://www.iba.org.in)

# About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list for the past 10 years, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

## Sandeep Gupta

Managing Director  
[sandeep.gupta@protivitiglobal.in](mailto:sandeep.gupta@protivitiglobal.in)  
+91 9702730000

## Vaibhav Koul

Managing Director  
[vaibhav.koul@protivitiglobal.in](mailto:vaibhav.koul@protivitiglobal.in)  
+91 9819751715

## Ajay Malik

Managing Director  
[ajay.malik@protivitiglobal.in](mailto:ajay.malik@protivitiglobal.in)  
+91 9987071312

## Sarita Padmini

Senior Director  
[sarita.padmini@protivitiglobal.in](mailto:sarita.padmini@protivitiglobal.in)  
+91 9953043552

## Sahil Chander

Senior Director  
[sahil.chander@protivitiglobal.in](mailto:sahil.chander@protivitiglobal.in)  
+91 8800490154

## Nagesh Akula

Senior Director  
[nagesh.akula@protivitiglobal.in](mailto:nagesh.akula@protivitiglobal.in)  
+91 9866694411

## Acknowledgement

Nitin Bharadwaj from our Security & Privacy practice has contributed to the publication led by Vaibhav Koul & Sarita Padmini.

## OUR RECENT REPORTS

### INSIGHT



Navigating Data Privacy  
in Digital India



### REPORT



State of Data Privacy  
in India



### REPORT



State of Data Privacy  
in India



### REPORT



AI Trends and  
Future Impact  
Industry Adoption &  
Insights



### WHITEPAPER



AI Driven Collections  
Strategy for  
Unsecured Lending



### WHITEPAPER



ML Model Validation  
Best-practice



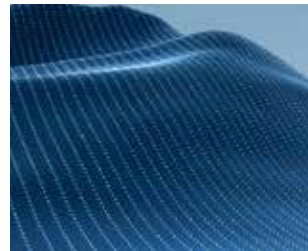
### INSIGHT



Top compliance  
challenges facing the  
technology industry  
in 2025



### INSIGHT



Technology-  
modernization  
projects



### NEWSLETTER



The Directors  
Playbook for Gen AI



### SURVEY REPORT



From AI To Cyber -  
Deconstructing  
A Complex Technology  
Risk Landscape



### INSIGHT



Harnessing the  
future: Protiviti's  
research on AI  
adoption





# PROTIVITI INDIA OFFICES

## Ahmedabad

6th Floor, West Gate, E-Block,  
Near YMCA Club, SG Highway,  
Gujarat, 380 015, India

## Bengaluru

Umiya Business Bay – 1, 9th Floor  
Cessna Business Park, Outer Ring  
Road, Kadubeesanahalli, Varthur  
Hobli Bengaluru – 560 049  
Karnataka, India

## Bhubaneswar

1st floor, Unit No 104, 105, 106  
Utkal Signature, Chennai Kolkata  
Highway Pahala, Bhubaneswar  
Khordha – 752 101  
Odisha, India

## Chennai

10th Floor, Module No. 1007  
D Block, North Side, Tidel Park  
No. 4, Rajiv Gandhi, Salai,  
Taramani, Chennai – 600 113  
Tamil Nadu, India

## Coimbatore

TICEL Bio Park, (1101 – 1104)  
11th floor Somaiyapalyam  
Village, Anna University Campus,  
Maruthamalai Road, Coimbatore  
North Taluk, Coimbatore – 641046  
Tamil Nadu, India

## Gurugram

15th & 16th Floor, Tower A,  
DLF Building No. 5, DLF Phase III  
DLF Cyber City,  
Gurugram – 122 002  
Haryana, India

## Hyderabad

Q City, 4th Floor, Block B,  
Survey No. 109, 110 & 111/2  
Nanakramguda Village  
Serilingampally Mandal, R.R.  
District Hyderabad – 500 032  
Telangana, India

## Kolkata

PS Srijan Corporate Park,  
Unit No. 1001 10th & 16th Floor,  
Tower – 1, Plot No. 2 Block – EP &  
GP Sector-V, Bidhannagar  
Salt Lake Electronics Complex  
Kolkata – 700 091,  
West Bengal, India

## Mumbai

1st Floor, Godrej Coliseum  
A & B Wing Somaiya Hospital Road  
Sion (East) Mumbai – 400 022  
Maharashtra, India

## Mumbai – Goregaon\*

The Westin Garden City,  
13th Floor, Commerz 1–  
International Business Park,  
Behind Oberoi mall, South Side,  
Goregaon, Mumbai – 400063,  
Maharashtra, India

## Noida

Windsor Grand, 14th & 16th Floor  
1C, Sector – 126 Noida  
Gautam Buddha Nagar– 201313  
Uttar Pradesh, India

## Face the Future with Confidence®

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the person listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti India Member Private Limited nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.

©2025 Protiviti India Member Private Limited

MS\_ 129284\_May2025