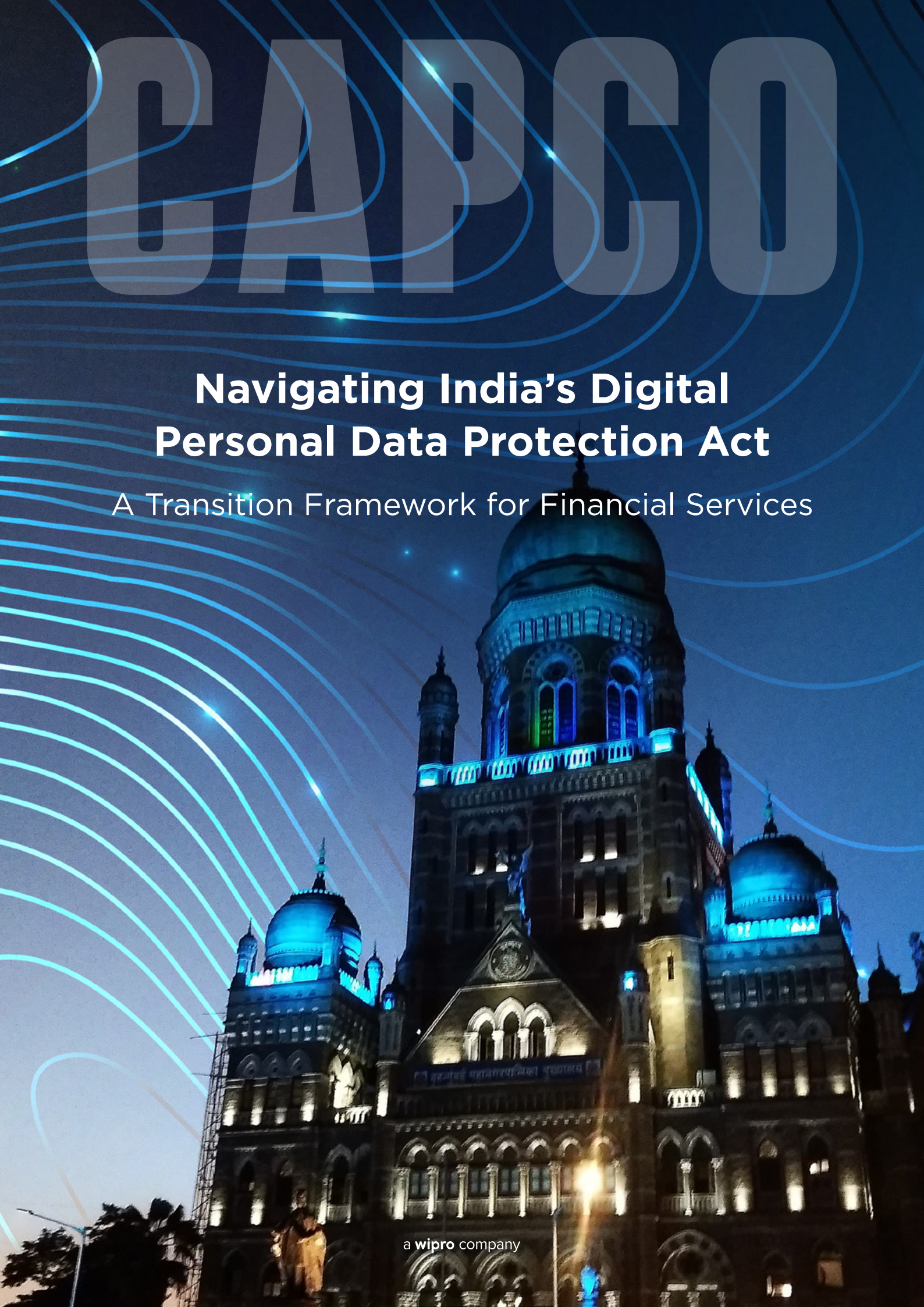
CAPCO

Navigating India's Digital Personal Data Protection Act

A Transition Framework for Financial Services



a **wipro** company

With the release in January of its draft Digital Personal Data Protection Rules, India's Ministry of Electronics and Information Technology (MeitY) has initiated the next step in the ongoing evolution of the nation's data protection framework. With a subsequent public consultation having closed in early March, we explore the implications for India's financial services industry and some key priorities for firms as they seek alignment with the new guidelines.

Emphasizing transparency, accountability, and lawful processing of digital personal data, the new Rules serve as an extension of India's groundbreaking Digital Personal Data Protection Act, 2023 (DPDPA), and provide much-needed clarity on the Act's implementation.[1] Shaping how businesses should collect, process, and safeguard personal data in the digital age, they mark a significant milestone in India's data protection journey.

> **For financial institutions that increasingly rely on digital data, understanding and adhering to these regulations is critical to maintaining consumer trust, regulatory compliance, and mitigating legal and financial risks.**

In this paper, we will navigate the key provisions of the DPDPA, its implications for financial institutions and fintechs, the challenges of compliance, and strategies for ensuring a smooth transition to the new regulatory framework.

1. https://dpdpa.com/index.html

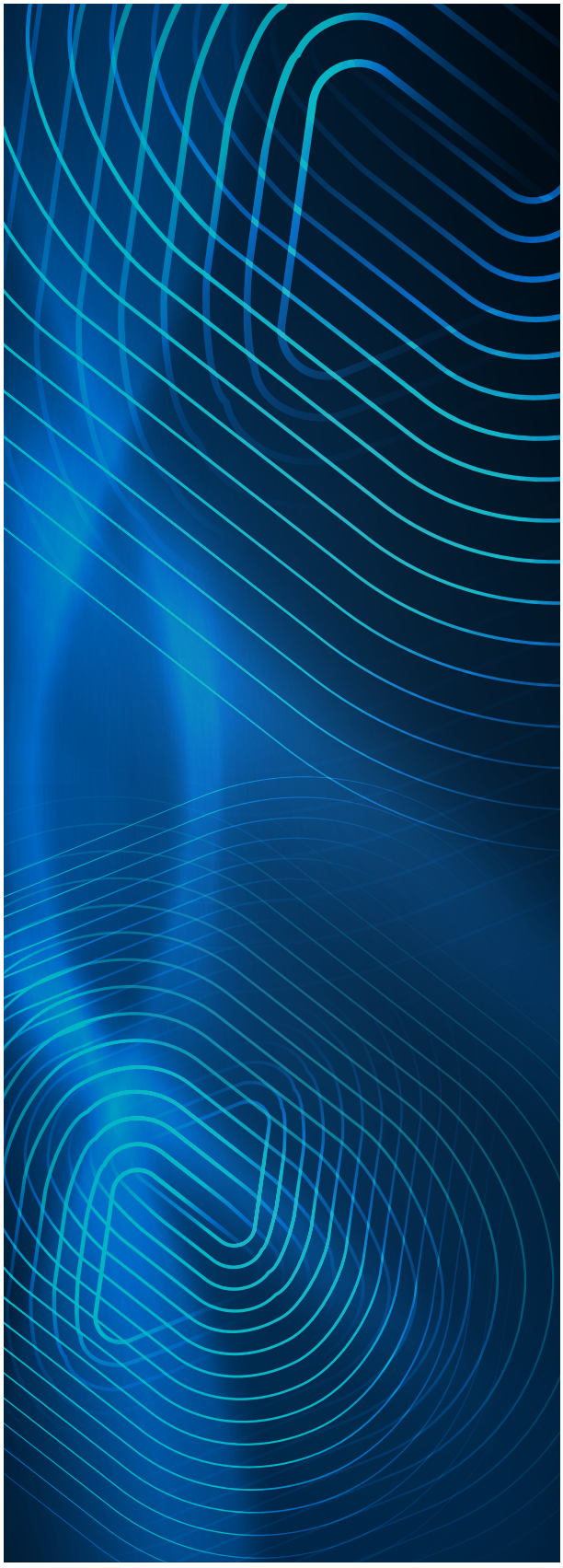
A milestone in data protection

As noted, the DPDPA represents a significant milestone in India's journey toward comprehensive data protection, aiming to balance individual privacy rights with lawful data processing needs.

The Act introduced key principles such as principle of consent, purpose limitation, data minimization, personal data accuracy, storage limitation, data safeguard, and principle of accountability, aligning with global standards like the GDPR while incorporating India-specific regulatory nuances.

Since its enactment, the regulatory landscape has continued to evolve. The latest draft DPDPA Rules, 2025, introduces several refinements to enhance compliance and implementation, including:

- **Data localization** – critical personal data must remain in India
- **Consent mechanisms** – ensuring users fully understand how their data is collected, processed, and shared
- **Enhanced transparency** – mandating detailed disclosures on data usage, storage, and retention policies
- **Right of Data Principals** – individuals can access their data, request corrections or deletions and file grievances with fiduciaries and escalate unresolved issues to the DP Board
- **Duties of Data Fiduciaries** – the Rules impose severe fiduciary obligations, such as:
    - security measures include encryption and access controls
    - carry out Data Protection Impact Assessments for significant data fiduciaries
    - establishment of grievance redressal mechanisms.



Impact on financial institutions and fintechs

The DPDPA 2023 introduced stringent data privacy and protection requirements for financial institutions and fintechs.

Increased obligations

- Greater focus on transparency, accountability, and customer control over personal data
- Compliance requires stricter data collection, processing, and security measures

Enhanced safeguards for sensitive data

- Stricter handling of financial information and medical records
- Compliance demands investment in new systems, and processes
- Marketing and customer engagement require explicit consent with opt-out rights

Customer service requirements

- Efficient handling of data access, correction, deletion and restriction requests
- Data retention policies must align with regulations, store data only as necessary
- Implement technical and organizational measures to prevent unauthorized access, use or modification

Fintech specific challenges

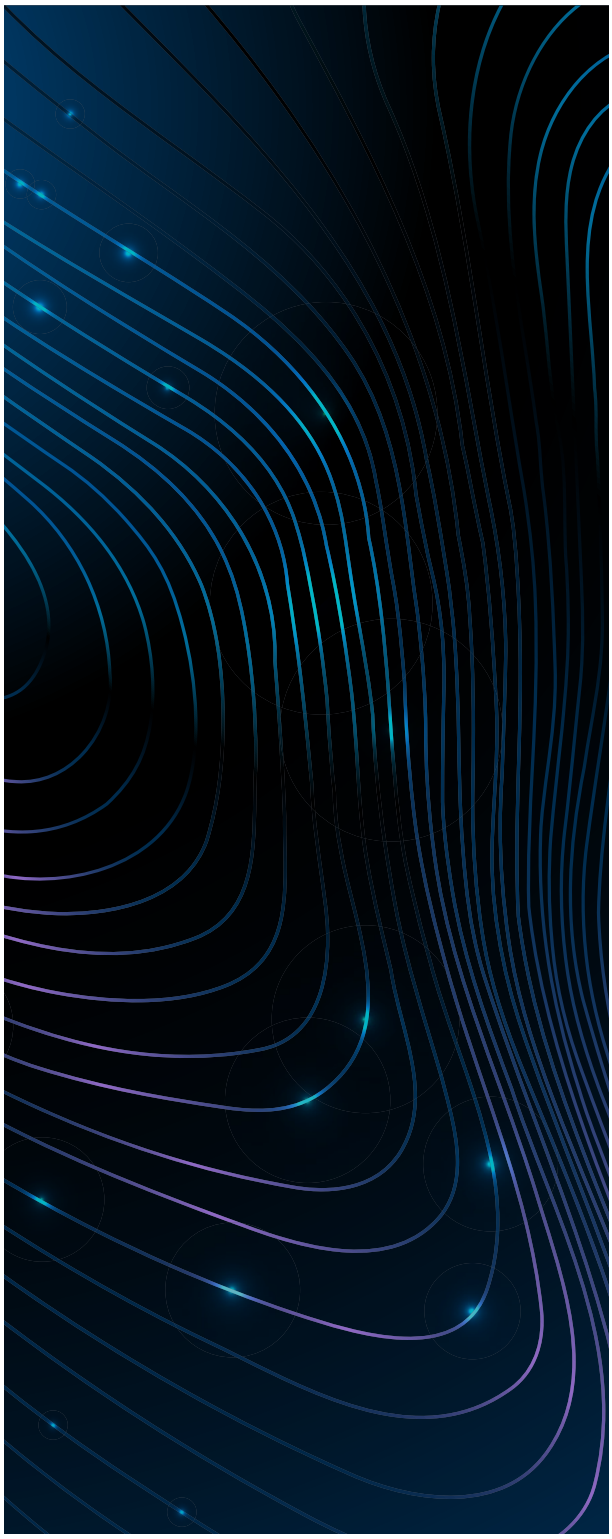
- Compliance with cross-border transfer regulations and security
- Appointment of Data Protection Officers (DPOs) for significant data fiducaries
- Require data inventory, mapping, minimization, purpose limitation and transparency

However, ensuring compliance will demand significant investments in new systems and processes, which is one of the biggest challenges for this industry. Fintechs, in particular, will need to invest in stronger compliance measures to meet these evolving requirements.

Organizations deemed to be 'high-risk entities' – including banks and fintech firms handling large volumes of sensitive personal data – will face heightened scrutiny and stricter compliance obligations.

Failure to comply could lead to significant financial penalties, with fines ranging from INR 10,000 for minor violations to INR 250 crores for severe breaches. Additionally, data breaches and non-compliance can erode consumer trust and brand value, with clear reputational implications.

Mixed reactions across financial services



While the proposed framework aligns with global data protection standards, industry leaders have highlighted implementation challenges, particularly for startups and MSMEs that may struggle with compliance costs.

The Internet and Mobile Association of India (IAMAI) has urged MeitY for a 24-month transition period to allow businesses adequate time for compliance.

Despite these challenges, the Rules represent a significant step in strengthening India's privacy framework. They bring India in line with global data protection norms while incorporating country-specific provisions. Although these regulations raise the bar on compliance, they also remove ambiguity for global businesses.

Companies already operating in India, or eyeing the market, must get ahead by thoroughly preparing for these robust requirements – building compliance into their strategy to ensure sustainable growth and success.

Other key concerns raised by industry include:

- **Operational burden** – financial institutions and fintech firms may need to enhance or revamp their existing data governance practices to align with compliance requirements
- **Cost implications** – compliance demands increased investment, including hiring data protection officers (DPOs) and upgrading security infrastructure
- **Impact on customer experience** – ensuring regulatory compliance while maintaining a seamless and user-friendly experience remains a challenge.

Key priorities for financial institutions

While financial institutions and fintechs across India are at different stages of readiness, adherence to some key principles can help firms smooth their path to DPDPA compliance. Below we set out the priority areas of focus to strengthen internal governance, ensure robust security measures, and foster a culture of data protection.

Comprehensive data privacy policy development. Establish clear, transparent, and legally sound privacy policies that outline how customer data is collected, processed, stored, and shared. Provide explicit guidelines on consent mechanisms, data retention periods, and user rights.

Implementation of strong data protection measures. Institutions must deploy rigorous access control and role-based authentication policies. Furthermore, the data minimization principle must be followed to collect only the required data for specific purposes.

Regular privacy audits and risk assessments. Financial institutions must conduct periodic audits and assessments to identify compliance gaps and security vulnerabilities. Key actions include:

- Data flow mapping to track the movement of personal data within the organization
- Vulnerability assessments to identify weaknesses in digital infrastructure
- Policy and procedure audits to verify alignment with data protection regulations
- Regular penetration testing to uncover potential security gaps.

Employee training and awareness. Developing a security awareness culture within the organization is critical to staying alert to data breaches and ensuring employees are able to meet privacy standards.

Robust vendor compliance mechanisms. As fintech partnerships and outsourcing grow, institutions must ensure third-party vendors comply with DPDPA regulations. This involves:

- Incorporating data protection clauses in vendor contracts
- Conducting due diligence to assess vendor security controls
- Setting up monitoring mechanisms to track vendor compliance with data handling requirements.

Data breach response planning. A well-defined incident response strategy that includes:

- A dedicated Data Protection Officer (DPO) to oversee compliance and breach management
- Incident response protocols for detecting, containing, and mitigating breaches
- Timely reporting mechanisms to notify the Data Protection Board and affected individuals within stipulated timelines
- Post-breach remediation measures to strengthen security and prevent recurrence.

Capco's three-step compliance framework

To navigate the Act's complexities, we recommend financial institutions and fintechs adopt a structured approach via a three-step framework.

Assess & strategize

The first step toward compliance is a comprehensive gap assessment that helps institutions understand where they currently stand and what changes are needed.

- **Gap & risk assessment** – conducting in-depth evaluations to identify compliance gaps, assess potential risks, and benchmark against regulatory expectations
- **Regulatory alignment** – defining key compliance objectives by answering the "why, what & how" of DPDPA.
  - Why is compliance critical for business continuity, trust, and regulatory adherence?
  - What specific data governance and protection measures are required?
  - How can these measures be effectively implemented within existing business operations?
- **Strategic roadmap development** – creating a customized, actionable roadmap that ensures a phased, structured transition towards full compliance, minimizing business disruptions.

Implement & govern

Once the strategic foundation is in place, financial institutions should implement robust governance structures and operational controls to ensure compliance sustainability.

- **Governance and accountability** – establishing a data governance framework that defines roles, responsibilities, and reporting mechanisms for compliance oversight
- **Technical & operational safeguards** – deploying advanced data security measures, including encryption, access controls, anonymization, and incident response mechanisms
- **Risk management & monitoring** – implementing proactive risk management strategies to identify and mitigate potential data breaches, non-compliance risks, and regulatory lapses
- **Compliance audits & controls** – establishing internal audit mechanisms to regularly assess and refine compliance measures, ensuring long-term adherence to DPDPA mandates.

Communicate & sustain

Regulatory compliance is not just a one-time effort but an ongoing process. Organizations can maintain compliance by fostering a culture of data protection through effective communication and training initiatives.

- **Internal & external communication strategy** – developing clear, concise communication plans to educate employees, partners, and customers about new data privacy policies and responsibilities
- **Training & awareness programs** – conducting regular workshops and training sessions to ensure employees understand DPDPA requirements, data handling best practices, and incident response protocols
- **Stakeholder engagement** – encouraging collaboration between internal teams, regulatory bodies, and industry peers to ensure best practices, compliance agility, and continuous improvement
- **Continuous compliance monitoring** – implementing compliance tracking mechanisms that adapt to regulatory changes, ensuring businesses remain compliant as laws evolve.

Navigating a paradigm shift in data protection

While DPDPA compliance presents challenges, a structured approach to compliance, focusing on transparency, accountability, and technological preparedness, can help financial institutions on the journey ahead.

As firms negotiate hurdles posed by operational adjustments, new security measures, and fresh financial investments, they should also view this as an opportunity to build trust, enhance data governance, and foster responsible customer service. Organizations that proactively adapt to these regulations will not only ensure compliance but also gain a competitive advantage in the evolving digital economy.

Capco brings deep expertise in compliance and regulatory transformation. Contact us to find out how we can help you meet the requirements set by the DPDPA.

Authors

Dipanjan Naha

Madhav Malhotra

Priya Mitra

Contact

Dipanjan Naha
Partner & Head of India Market
dipanjan.naha@capco.com

Madhav Malhotra
Partner & APAC Capital Markets Lead
madhav.malhotra@capco.com

About Capco

Capco, a Wipro company, is a global management and technology consultancy specializing in driving transformation in the energy and financial services industries. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on LinkedIn, Instagram, Facebook, and YouTube.

Worldwide Offices

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurgaon
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST
Dubai

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto

SOUTH AMERICA
São Paulo

CAPCO.COM

CAPCO
a wipro company