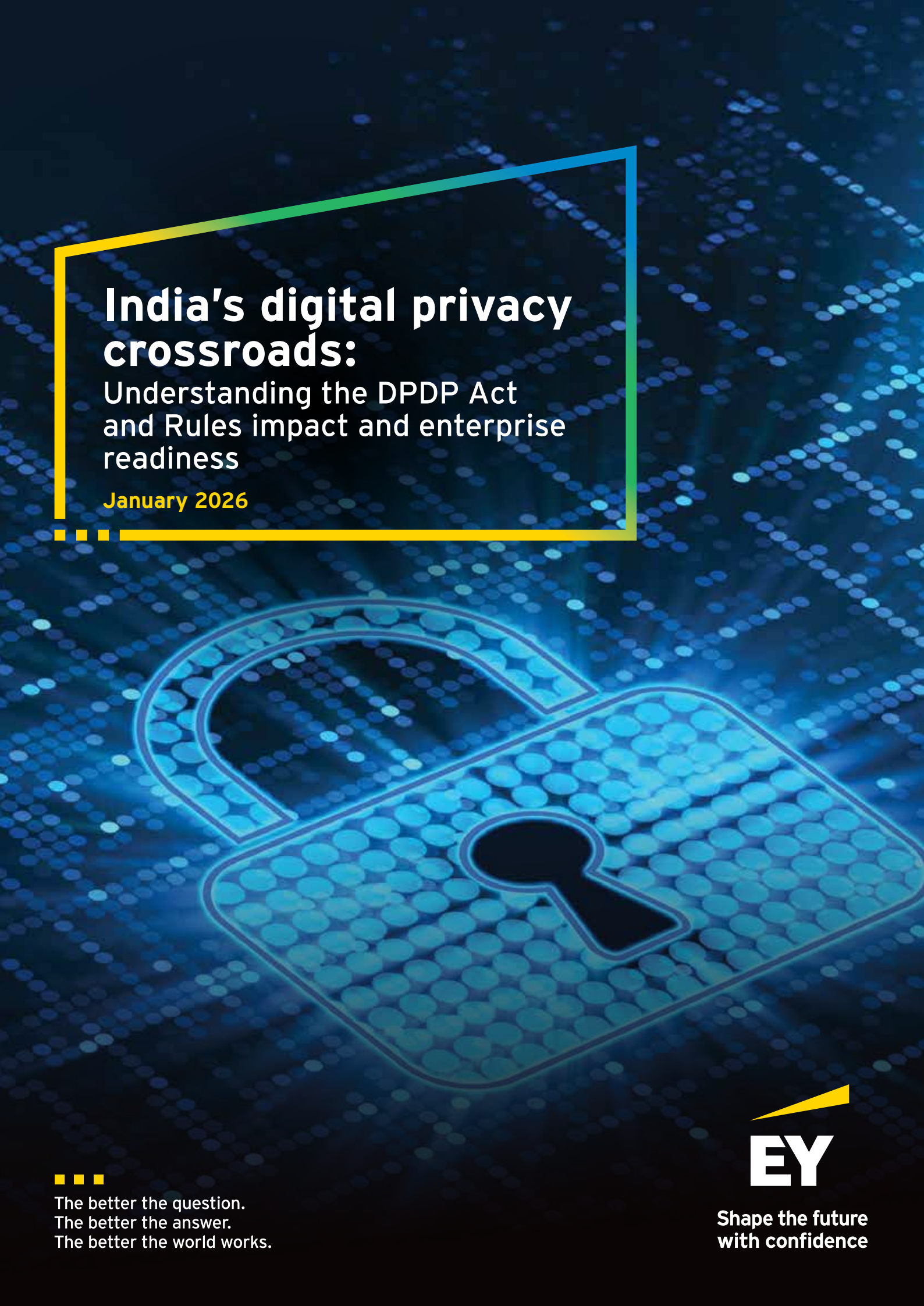
India's digital privacy crossroads:

Understanding the DPDP Act and Rules impact and enterprise readiness

January 2026



The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

Contents

In a landscape defined by decentralized data flows, algorithmic processing, and growing reliance on third party service providers, compliance with the DPDP Act and Rules is evolving from a legal mandate into a foundational design principle for enterprise digital systems. The Act's focus on consent driven processing, purpose limitation, and Data Principal rights requires a fundamental reassessment of existing system development and data management approaches.

Organizations must modernize their data architectures by integrating consent management, data governance models, automated classification, and continuous oversight. Early adoption not only enables privacy by design and policy as code automation but also minimizes risk and strengthens transparency and accountability.

Rohan Sachdev
Consulting Leader,
EY India

Foreword

India's electrifying advancement in digital technology makes the Digital Personal Data Protection Act (DPDP Act) and its accompanying Rules, a defining milestone, one that seeks to balance innovation with strong and enforceable privacy provisions. The Act outlines basic principles such as explicit consent, withdrawal rights and organizational accountability, which forms an important structure for dealing with personal data across industries. It is not just another Act and set of rules; they represent a paradigm change in the way we approach personal data management.

The impact of the DPDP Act and Rules varies across sectors due to differences in data maturity, governance, and operational readiness. EY surveyed professionals across industries to understand how organizations in sectors such as financial services, technology, consumer and retail, healthcare, manufacturing, telecom, media and entertainment, education, and automotive are approaching compliance at different stages. This report explores how these different sectors, especially those managing complex operations, workforce and infrastructure landscape, are preparing for this shift. Many companies have already initiated early measures to achieve compliance, but a significant number still struggle with understanding the nuances of the Act and its operational implications. The level of awareness varies across sectors, which clearly highlights an opportunity for industry bodies to create awareness about DPDP Act and Rules and its implications, within their respective sectors and for organizations to build capacity in terms of people, process and technology to enable compliance. Organizations are increasingly balancing internal capability building with external subject matter expertise to navigate the compliance requirements effectively.

Companies now have to decide whether to tick the regulatory boxes or achieve stronger data protection standards through architectural design changes that benefit the cause. Internally, they need to question if their processes align with the required regulations, will their systems still protect the data at par with the leading practices and industry standards?

If the answer is yes, they truly have attained practical compliance.

Organizations must recognize that compliance with the DPDP Act and Rules is a cross-functional responsibility, requiring active participation from key departments. Successfully embedding privacy into daily operations will require governance, accountability, close collaboration and support from key functions like legal, technology, cyber security, risk and business teams and organization wide cultural shift to manage data responsibly.

DPDP Act and Rules is no longer a legal milestone to achieve but an eye opener to the practices the organizations have adopted and whether they really demonstrate transparency to induce trust and accountability in their practices to build systems that are both resilient and respectful of an individual's autonomy.

A proactive approach to the DPDP Act and Rules will do more than meeting regulatory timelines, it will create lasting trust with customers, employees and other business stakeholders, reduce concerns about compliance related uncertainty and create a powerful competitive advantage in increasingly data driven market.

This report aims to provide decision-makers with clear and practical roadmaps on how to embark on the journey of DPDP Act and Rules while striking a balance between compliance and business priorities.

Murali Rao
Partner and Leader,
Cybersecurity Consulting,
EY India

Mini Gupta
Partner, Cybersecurity and
National Leader-Data Privacy,
EY India

Lalit Kalra
Partner, Cybersecurity and
National Leader-Data Privacy,
EY India

Executive

With the Digital Personal Data Protection Act (DPDP Act), 2023, now fully in force and the Digital Personal Data Protection Rules (DPDP Rules) notified on 13 November 2025, Indian enterprises have decisively shifted from planning to execution. The DPDP Rules introduced a phased compliance runway with immediate establishment of Data Protection Board (DPB) and its obligations, followed by Consent Manager registration and obligations within a year and Data Fiduciary related obligations taking effect within 18 months from the date of DPDP Rules being published. The Rules deliver long-awaited specificity and provide actionable clarity: clear and prospective privacy notice standards, a mandatory 90-day grievance redressal timeline, defined breach-reporting duties and one-year log-retention requirements for the purpose of state security, legal compliance and oversight. Together, the Rules convert the Act's principles into an operational playbook for organizations.

The impact of the DPDP Act and Rules varies across sectors due to differences in data maturity, governance, and operational readiness. EY surveyed professionals

Regulatory-mature sectors such as financial services and IT are expected to lead adoption, using and enhancing their existing governance models and compliance capabilities and are likely to set the pace for industry-wide adoption. In contrast, entities from sectors such as healthcare, manufacturing, shipping, metals, education and insurance are grappling with moderate to low readiness. While many companies have initiated foundational activities, such as conducting gap assessments, identifying and documenting personal data inventory, mapping data flows and identifying processing activities, additional and more advanced capabilities remain limited. These include establishing privacy framework, formalizing policy and procedures, establishing third-party privacy risk management practices and operationalizing personal data protection controls.

While the DPDP Act and Rules serves as the overarching framework for personal data processing, sector-specific regulations from authorities such as the Telecom Regulatory Authority of India (TRAI), the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), healthcare-related bodies, etc. remain essential.

summary

These sectorial guidelines define expectations for individual sectors and complement the broader principles established by the DPDP Act and Rules. For organizations looking to strengthen their data protection strategies, it is crucial to understand how these regulations intersect and influence one another.

An effective compliance roadmap begins with establishing a dedicated data privacy and data protection focused function, driving organizational awareness and identifying regulatory gaps. This can be followed by mapping and classifying personal data, including third-party system and cross-border flows, then implementing dynamic consent mechanisms, Data Principal rights workflows and child data safeguards where relevant. Strong governance must be anchored through breach response policies, grievance procedures, security controls and vendor agreements with proper documentation. Conducting a privacy risk assesment and breach simulation exercises build operational readiness. Ongoing success and sustained compliance will depend on continuous policy update, refresher training for staff and staying audit ready as regulations evolve.

In the end, privacy is no longer a check-the-box compliance obligation; it is a strategic and competitive differentiator. Businesses that proactively embed privacy by design into their data strategy and operations are better positioned to win customer trust, attract global partners and scale responsibly and confidently in a data-driven economy.

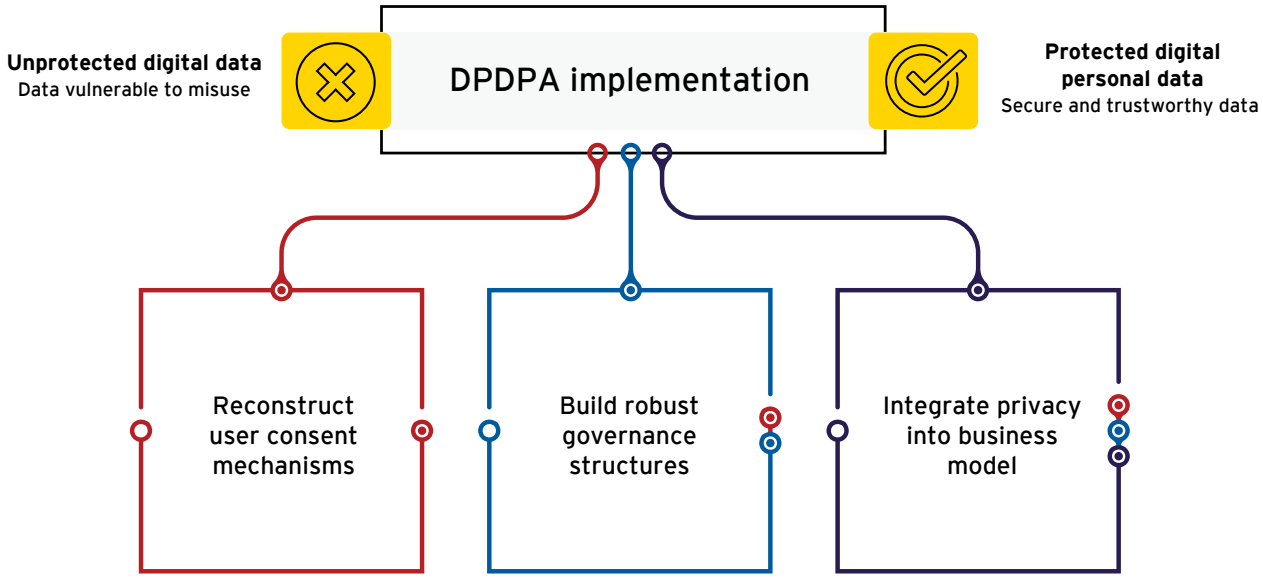
Section 1

Introduction

India stands at the crossroads of digital transformation, being one of the fastest-growing digital economies with widespread adoption of digital services in fintech, e-commerce and digital services among its young population. This transformation demands a comprehensive data protection policy and framework that fuels innovation while also safeguarding individual's privacy rights. The DPDP Act and Rules aim to establish this balance.

For businesses, the Act, however, introduces both opportunities and obligations as they prioritize privacy as a strategic factor. Trust is emerging as a competitive advantage; organizations that effectively implement privacy frameworks are not only better positioned to meet compliance but also likely to gain customer confidence, strengthen brand integrity and enhance operational efficiency. Seen through this lens, the DPDP Act and Rules can be viewed as an enabler of positive change in India's digital economy rather than just a regulatory requirement. While achieving compliance requires effort, it can ultimately lead to clarity and long-term, trust-based data relationships that yield tangible benefits.

Shows how organizations are balancing innovation with privacy rights under the DPDP Act and Rules



India's Digital Personal Data Protection Act

As India accelerates its digital transformation journey, DPDP Act and Rules establishes fundamental guidelines for personal data governance. Anchored in principles of robust personal data protection of individuals, combined with clear requirements for companies managing personal data, the Act makes a decisive shift in how personal data is managed across sectors.

Core requirements of the DPDP Act and Rules

The Act operates on several fundamental requirements that reshape personal data governance practices:

Explicit consent framework

Businesses are required to obtain explicit and affirmative consent to process personal data. Commercial entities, therefore, may need to redesign their approach to obtaining and managing Data Principal consents accordingly. Organizations must review historical data collection practices to confirm whether valid consent exists. If prior obtained consent already meets the Act's standards, no re-consent is needed. However, if consent was never obtained, is incomplete, or does not align with the Act's requirements, providing updated notices and obtaining fresh consent become mandatory. Additionally, the Act requires organizations to focus on redesigning consent journeys, modernizing interfaces and ensuring obtained consent is meaningful and truly empowers the Data Principals.

Data Principals rights

The Act grants complete authority to Data Principals to manage their personal data through the following rights:

- Right to transparent access to their data
- Right to correct inaccuracies, data deletion under specified conditions
- Right to nominate another person to act on their behalf in the event of their death or incapacity
- Right to grievance redressal

- Right to withdraw their consent for processing of data for the specified purpose

Businesses would need to develop appropriate and scalable frameworks, models, mechanisms and processes to respond to these Data Principal requests according to the provisions effectively and within defined timelines.

Breach management

In the event of a breach, the DPDP Act and Rules mandates reporting to the Data Protection Board (DPB) and the impacted Data Principals without undue delay, followed by a detailed report to the DPB within 72 hours of observing the data breach incident. Companies would therefore need to establish protocols for:

- Timely notification to affected parties
- Disclosure to DPB
- Implementation of corrective actions

These requirements translate long-standing security best practices into explicit formal compliance expectations.

Significant Data Fiduciary (SDF) compliance requirements

The Act uses factors such as data volume, sensitivity and organizational role to determine whether an entity qualifies as an SDF and to define its essential obligations. All designated entities qualified to be SDFs are required to appoint Data Protection Officers (DPOs) who have the following responsibilities:

- Ensuring internal compliance
- Serving as a point of contact with the regulatory authorities and the Data Principals
- Promoting privacy awareness within the organization
- To ensure data protection oversight, in accordance with this requirement.

Additionally, SDFs are also required to appoint an independent auditor to carry out annual data privacy audits, evaluate the organization's compliance with the regulatory obligations and conduct annual Data Protection Impact Assessments (DPIA) to identify and mitigate any risks to the rights of the Data Principals. The key findings from the audit and DPIA must be reported to the DPB by the SDFs. These requirements set up a structured framework for data protection continuous oversight, enabling SDFs to maintain a proactive and demonstrable commitment to privacy compliance. While it is not clear who will get notified to be an SDF, however, clearly there will be an increased focus and scrutiny on these entities once notified. Basis our point of view, large banks, insurance companies, telecom operators, large hospitals, etc., may get notified to be SDFs and hence can benefit from proactively preparing to comply with the obligations of an SDF.

Data Protection obligations across types of organizations

Business-to-Business (B2B) companies share significant responsibility for protecting personal data, even when their primary customers are other businesses. In every B2B engagement, personal data – such as employee details, user credentials, vendor information – is inevitably processed. Additionally, they may also be processing clients' end-customers' personal data. Obligations around transparency, purpose limitation, security safeguards and responsible data sharing apply. With B2B vendors sitting deep inside a client's technology stack or business flow, even a single lapse can impact multiple organizations and their users, which makes strong data governance, privacy-by-design, minimum security safeguards and demonstrable compliance essential. Ultimately, B2B companies must treat data privacy as a core accountability and not merely a contractual formality.

Business-to-Consumer (B2C) companies carry an even more heightened responsibility for protecting personal data because they interact directly with individuals whose privacy expectations, rights and vulnerabilities are greater. These organizations typically collect higher volumes of personal and identity information, contact details, behavioral insights, transaction histories, preferences and consent logs. This increases expectations around transparent notices, valid and granular consent, purpose limitation, data minimization, secure processing, defined retention policies and mechanisms to honor individuals' rights (access, correction, erasure, grievance redressal). B2C entities must also manage higher regulatory scrutiny, heightened risk of individual harm and the need for strong customer-facing privacy practices.

Digital Personal Data Protection Rules

With the final DPDP Act and Rules now officially notified, India has entered the implementation phase. The Rules provide the operational clarity that organizations had been awaiting and formally begin the 18-month compliance window.

Enforcement timeline

The enforcement timeline is structured across three phases:

- **Immediate (effective 13 Nov 2025) –** Establishment of the DPB and commencement of associated obligations.
- **Within one year of publication of Rules –** Registration and obligations for Consent Managers.
- **Within 18 months of publication of Rules –** Compliance with Data Fiduciary obligations.

The Rules set out detailed expectations for clear and prescriptive privacy notices, consent lifecycle management, withdrawal pathways, 72-hour breach reporting, one-year log retention and minimum-security safeguards. They also mandate a 90-day grievance-redressal timeline, establishing clear timelines for response and accountability.

The Rules further outline the additional obligations of SDFs including annual audits and DPIAs, algorithmic risk reviews and strengthened governance expectations. They also establish the operating framework for Consent Managers, setting out registration requirements and standards for seamless, interoperable consent management for Data Principals.

Cross-border transfers are not permitted to jurisdictions that are not approved by the central government, while SDFs face additional localization and transfer restrictions on certain categories of personal and traffic data that may be notified. This will require reassessment of data-flow architectures, systems, vendor landscape, contracting structures and global delivery models in data-intensive sectors.

Data Processors, while not directly regulated, must contractually support reasonable security safeguards, one-year log retention, breach-reporting support and strict alignment with the Data Fiduciary's purpose and retention limits. This meaningfully elevates accountability for IT, BPO, SaaS and managed service providers operating under fiduciary instructions.

With clarity available, organizations are transitioning from planning to execution. The critical focus is on building scalable systems that can manage consent, automate retention, enable security logging, support grievance workflows and coordinate breach response. This demands tight collaboration between legal, technology, cybersecurity, product and vendor-management teams, making privacy transformation an enterprise-wide agenda rather than a compliance exercise.

The next few months till May 2027 will be a period of intensive operationalization and continued practice. Enterprises must modernize legacy platforms, digitize manual data practices, embed privacy controls into core delivery workflows, refresh contracts and strengthen audit readiness. Organizations that approach DPDP implementation as a structural upgrade, rather than a regulatory obligation, will emerge with stronger governance.

Strategic implications

The DPDP Act and Rules represent more than regulatory obligations; they shape how enterprises compete, operate and build trust in a digital economy. They set up data protection requirements that can affect operations, leading companies to treat data protection as a necessary legal standard and an essential business priority. Actively implementing these modifications would allow companies to build trust with consumers while establishing compliance as a strategic business and competitive advantage.

Organizations operating across multiple countries must comply with the data protection regulations of each jurisdiction, which, while presenting compliance challenges, are a regulatory necessity. Adherence to these standards is essential for global alignment, trust-building and the facilitation of streamlined cross-border data flows, the attraction of international partners and investors and the support of scalable global operations. Non-compliance with the DPDP Act and Rules may lead to substantial financial penalties, harm to reputation, risk of business disruption and increased regulatory scrutiny. These risks further highlight the importance of proactive

preparedness and effective governance.
India is at the fulcrum of digital transformation and through this Act, aims to achieve a balance between innovation and the protection of Data Principal rights. Appropriate implementation of this Act necessitates collaboration between the business, regulators and the public to develop a privacy-based data system that promotes India's digital transformation agenda in a responsible way.

Interpretation to execution

With the final DPDP Rules notified and the compliance window formally underway, organizations can no longer rely on a wait-and-watch approach. The period of uncertainty that accompanied the draft rules has ended. Regulatory expectations are now explicit. Enterprises that had paused major activities such as detailed gap assessments, personal data inventories and systems remediation must now accelerate these efforts to align with the 18-month implementation timeline.

Third-party governance is also moving to the forefront. Many organizations had previously identified their external vendors but had not completed privacy risk assessments or executed updated contractual safeguards. The final Rules make it clear that Data Fiduciaries are accountable for ensuring that all Data Processors implement required security controls, retention schedules, log-maintenance obligations and breach-reporting processes. This raises the urgency of conducting structured third-party assessments and formalizing Data Processing Agreements to mitigate downstream compliance risk.

Similarly, critical activities such as establishing a formal privacy governance structure, identification of data-collection touchpoints requiring notice or consent and the development of integrated operational policies had been deferred by several smaller companies pending regulatory clarity. With the Rules now final, these actions must be prioritized. Organizations will need to adopt a sequenced implementation plan — gap assessment, mapping data flows, establishment of policies and procedures, embedding consent and retention controls, updating notice mechanisms, conducting training and awareness and ensuring sustained rollout and monitoring.

The shift is clear: the DPDP Act and Rules has moved from interpretation to execution and organizations that proactively advance their compliance programs now would be far better positioned to meet regulatory timelines and can build enduring trust with their stakeholders.

Section 2

Survey

From compliance to confidence: Survey insights

The implications of the DPDP Act and Rules differ significantly across sectors driven by varying levels of data maturity, governance and operational readiness among companies. To examine the same, EY surveyed nearly 150 professionals, including senior leaders, mid-level managers and executives across various industries, providing a comprehensive understanding of the diverse approaches companies are adopting at various organizational levels. This survey reflects a cross section of perspectives from different organizations including financial services, technology services, consumer and retail, healthcare, manufacturing, telecom, media and entertainment, education, auto mobility and many others at different stages of their compliance journey.

The broad representation of this survey offers a comprehensive view of DPDP Act and Rules readiness across India's key economic verticals.

Familiarity with the DPDP Act and Rules and the Implementation Rules (November 2025)

General awareness is high but uneven

30%

The survey reveals varied levels of understanding among participants regarding the DPDP Act and Rules. Approximately 30% have moderate or lower awareness of the Act and its implications, highlighting significant gaps in knowledge at both leadership and execution levels.

Despite this, India Inc. is clearly mobilizing and preparing for compliance with the Act, as it becomes a key business imperative, though the levels of impact, maturity in readiness and implementation vary across sectors.

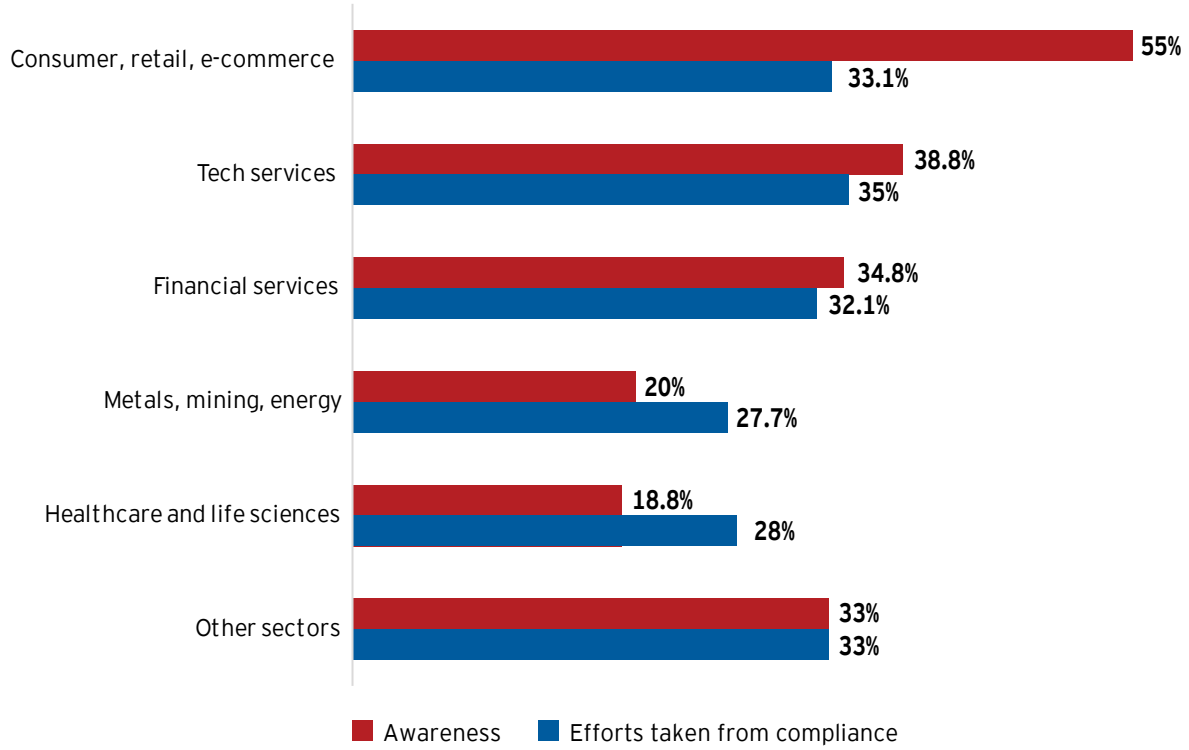
Industry awareness and compliance efforts towards DPDP Act and Rules

Sectors with a high degree of customer interaction or heavy reliance on customer data are likely to see the most impact of the DPDP Act and Rules. However, the level of awareness among such sectors differs significantly at present. For instance, companies in financial services and tech services have elevated awareness due to their high use of customer data and digital systems and already regulated landscape or governed by contractual and global compliances, leading them to adopt stronger data governance practices. Conversely, companies in the healthcare, metals, education sector, etc. have lower familiarity with the Act with the newly notified Rules, which translate the Act's principles into actionable requirements.

Some organizations in these sectors are preparing for compliance, while many others remain at a level of basic understanding of the Act's implications. Given the varying levels of understanding, greater effort is required to increase internal awareness and employee training and to develop policies around data protection and identifying and documenting personal data.

Among the sectors surveyed, manufacturing, infrastructure and shipping displayed the least familiarity with the DPDP Act and Rules. These industries are often characterized by legacy systems, limited digitization or narrower regulatory exposure. To bridge this knowledge gap, targeted support and public awareness programs are essential, to overcome compliance challenges.

Industry awareness and compliance efforts towards DPDP Act and Rules



Other sectors include manufacturing, media and entertainment, auto and mobility, telecom, education, hospitality, infrastructure, and government

Source: EY Research

Awareness levels across functions

Within organizations, it is important to understand the level of awareness among employees at different levels to identify the areas of strength and the existing gaps. Such insights can, in turn, lead to tailored and role-based training, effective communication and allocation of resources with the aim of strengthening compliance and building an overall culture of being highly aware of data privacy.

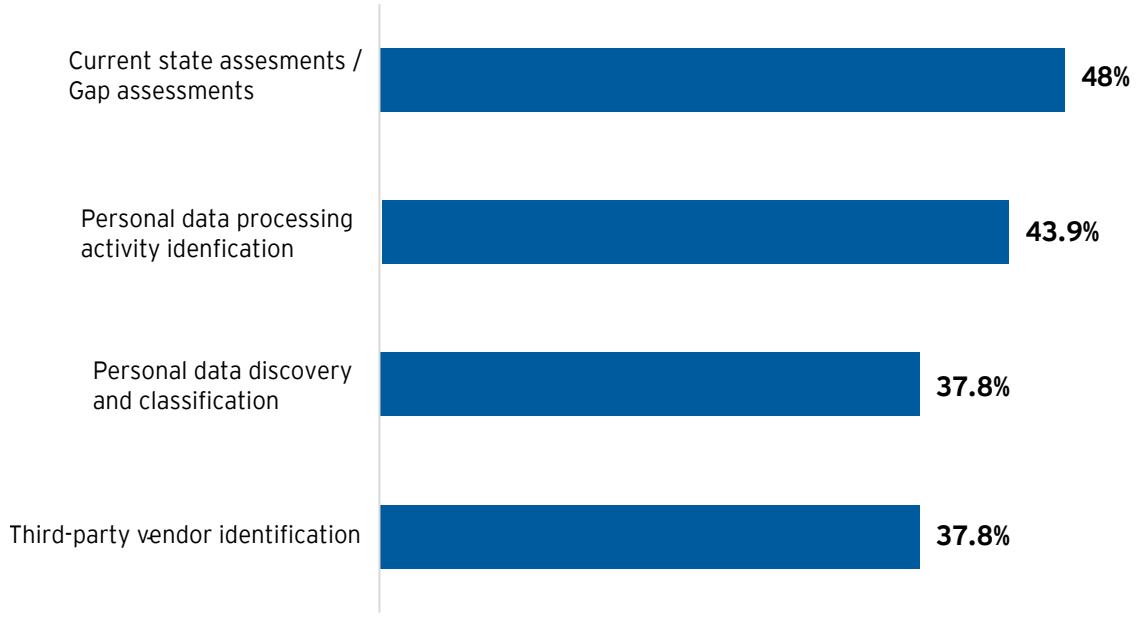
Functions directly engaged in compliance such as legal, cybersecurity and risk management exhibit higher awareness due to their inherent role in interpreting and managing regulatory requirements. Technology and Information Security teams also demonstrate strong awareness, as data privacy aligns closely with their existing responsibilities in cybersecurity. In contrast, operational functions like HR, Finance, Manufacturing and Business Operations exhibit significantly lower levels of awareness. Although these teams routinely handle personal data, they may lack dedicated training or clarity on privacy responsibilities, posing potential compliance risks.

The gap highlights the need for organization-wide privacy education, consistent awareness campaigns and stronger cross-functional coordination to enable full compliance with the DPDP Act and Rules.

Early stage prioritisation under DPDP Act and Rules compliance

While organizations are at varying maturity levels in their efforts to comply with the DPDP Act and Rules, however, most organisations have started focusing on key areas as indicated in the graph below.

Organizational progress in DPDP Act and Rules compliances



Source: EY Research

Close to 50% organizations have undertaken the first step of conducting a gap assessment, while the other compliance activities would follow.

Low priority areas in DPDP Act and Rules compliance are evident in several critical activities that organizations have not widely adopted:

80% **Policy updates and privacy governance structure:** About 80% of organizations have not initiated drafting or updating their policies and framework in line with the DPDP Act and Rules.

81% **Establishment of privacy governance structure:** About 81%, have not begun establishment of privacy governance structure and corresponding roles and responsibilities.

83% **DPDP Act and Rules implementation:** More than 83% organizations have not yet initiated implementation across relevant processes and systems.

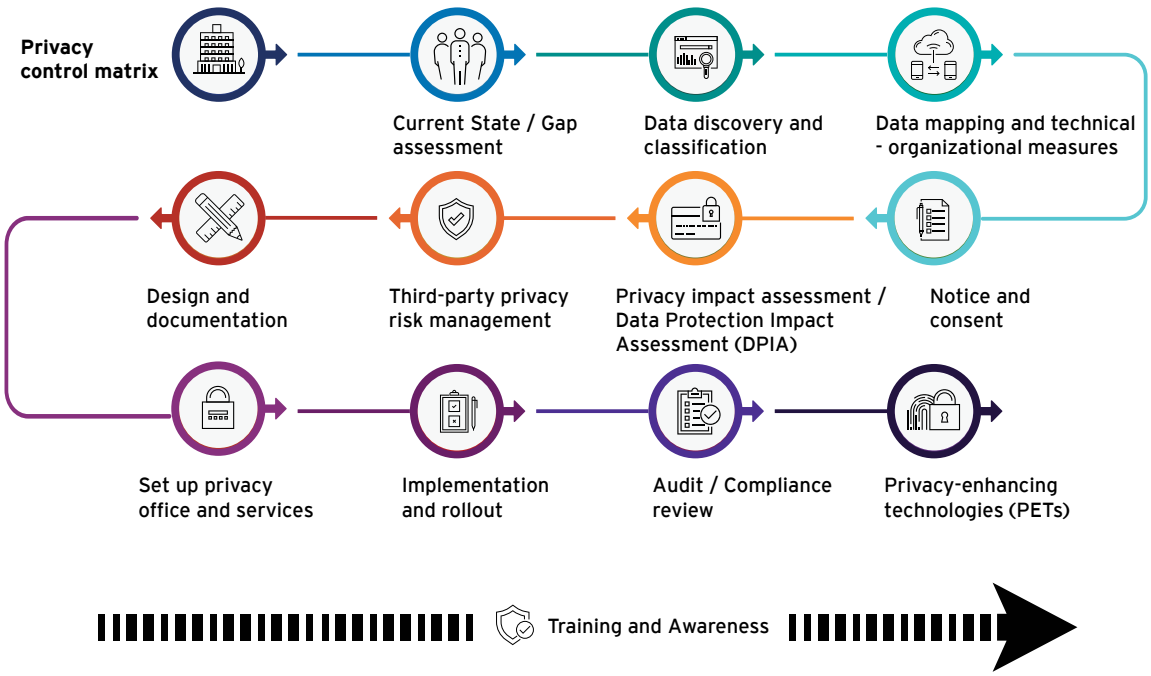
Currently, many organizations are focusing on achieving initial compliance maturity before addressing advanced requirements. Therefore, some activities, such as third-party privacy risk assessments and periodic privacy audits, are largely not undertaken across sectors.

Sector-wise awareness and maturity

- Financial services, consumer and retail, e-commerce and technology services: These sectors have made more substantial progress than others in core compliance tasks, including gap assessments, data flow mapping and processing documentation. Their advantage stems from higher regulatory exposure, client obligations, data governance frameworks and greater investments in privacy readiness.
- Sectors like education and healthcare: They face more pronounced challenges and show limited progress across most compliance areas. One of the biggest barriers include highly sensitive personal data spread across fragmented systems and legacy infrastructure. Combined with constrained budgets and limited in-house expertise, these factors delay structured adoption of privacy practices.

Suggested approach: To address the challenges and accelerate readiness, organizations can prioritize streamlining high-risk data flows, investing in centralized data governance and phasing compliance efforts in line with operational realities. Collaboration with industry associations and leveraging modular privacy tools can also reduce the burden of managing complex compliance requirements.

Illustrative roadmap to ensure compliance to Act and its Rules



Data protection readiness and progress in meeting DPDP Act and Rules requirements

Strong data protection practices enable organizations to safeguard the confidentiality, integrity and availability of personal data throughout their lifecycle. These requirements can be structured into Basic, Intermediary and Advanced levels , allowing organizations to build capability in a phased and scalable manner. Each tier strengthens governance, operational resilience and the ability to prevent unauthorized access, detect anomalies, respond to incidents and maintain operational resilience.

1. **Basic requirements** constitute the mandatory controls that every Data Fiduciary and any Data Processor acting on its behalf must implement for secure and accountable personal data processing. At a minimum, organizations must:

    - Implement appropriate data security measures such as encryption, masking, obfuscation, tokenization, or similar techniques.
    - Establish strict access controls to systems and computer resources so that only authorized personnel (including processors) can access personal data.
    - Maintain visibility into access and processing activities through logs, monitoring mechanisms and periodic reviews, enabling detection, investigation and remediation of unauthorized access.
    - Enable continuity of processing in case of a breach of confidentiality, integrity, or availability, including appropriate data-backup mechanisms and recovery procedures.
    - Retain relevant logs for at least one year.
    - Ensure contracts with Data Processors impose obligations to implement reasonable security safeguards consistent with the Act.
    - Conducting periodic vulnerability assessments, configuration reviews and security audits.
    - Adopt other suitable technical and organizational measures to implement required safeguards effectively and prevent recurrence of security failures.

2. **Intermediary requirements** go beyond statutory minimum to strengthen and operationalize protections by establishing structured governance, expanded monitoring and systematic security practices. These also represent good industry practices for organizations with growing data volumes or operational complexity. Typical additional expectations include:
    - Implementing data classification-based controls, including structured encryption policies, tiered access and defined retention rules.
    - Deploying formal information security policies, standards and role definitions (e.g., data owner, custodian, approver).
    - Strengthening identity and access management, including privileged access restrictions and periodic access-recertification.
    - Enforcing Secure Development Life Cycle (SDLC) practices, change management and timely patch management.
    - Establishing formal backup-testing routines, secure data-transfer protocols and environment segregation (dev/test/prod).
    - Implementing more structured logging, anomaly detection and incident-reporting workflows with defined responsibilities and SLAs.

3. **Advanced requirements** reflect mature, predictive and intelligence-driven protection capabilities. These measures are expected in data-intensive or highly regulated environments where proactive risk reduction is critical. Advanced practices additionally include:

    - Deploying advanced cryptographic controls, enterprise-grade key-management systems and organization-wide Data Loss Prevention (DLP) implementations.
    - Adopting Zero-Trust Architecture principles, including continuous identity verification, micro-segmentation and strict least-privilege enforcement.
    - Automating retention, deletion, archival and backup processes, including versioning and immutable storage.
    - Conducting regular penetration testing, red-team exercises, adversarial simulations and continuous security validation.
    - Establishing geographically distributed disaster-recovery environments and robust business-continuity scenarios.
    - Embedding security-by-design in architecture, procurement and development processes.
    - Instituting board-level oversight, security-risk reporting and integration of data-protection metrics into enterprise risk management.

Most organizations currently operate at a basic or intermediate stage of maturity concerning data protection standards. While their existing safeguards show reasonable effectiveness, there is potential for achieving higher maturity. There is progressive improvement, however, many organizations are still in the early stages of meeting compliance requirements of the DPDP Act and Rules.

The following insights highlight several important patterns regarding importance of data protection practices:

1. **High maturity levels in foundational data security controls:** Organizations demonstrate higher adoption of basic access controls, reflecting a foundation in traditional security practices. Security monitoring emerged as one of the most implemented protection measures, indicating a relatively higher awareness of basic security requirements.

   Suggested approach: While organizations show adoption of basic access control, they need to conduct a data discovery exercise to understand their personal data exposure and accordingly strengthen access governance. This includes identifying where personal data resides, classifying it based on sensitivity, and aligning access permissions with business roles and data criticality

2. **Lower maturity:** The maturity level in embedding security clauses within contracts and advanced data security measures such as obfuscation, masking, or virtual tokens for personal data protection, remains relatively low.

   Suggested approach: Prioritized risk-based rollout of advanced data protection measures, such as masking, obfuscation, or tokenization should be implemented for high-sensitivity personal data to improve overall security maturity. In order to implement these controls, it is necessary for organizations to have visibility around their personal data for which solutions around automated data discovery and data classification can be considered.

3. **Data retention requirements:** Under the DPDP Act, data retention is inherently purpose driven, requiring Data Fiduciaries to retain personal data only for as long as it is necessary to fulfill the specified purpose for which the data was collected. Once the purpose has been achieved or is no longer relevant, personal data must be erased unless continued retention is justified by legitimate business needs, compliance with other applicable laws, or as notified by the government. The Act and Rules require e-commerce entities and social media intermediaries with at least 2 crore registered users in India, as well as online gaming intermediaries with at least 50 lakh registered users in India, to retain data for a period of three years from the date on which the Data Principal last approached the Data Fiduciary to perform the specified purpose or to exercise her rights, or from the commencement of the Rules —whichever is later. After this period, the Data Fiduciary must ensure that such personal data and related logs are erased, unless further retention is required to comply with any other applicable law or as notified by the government.

   It was observed that organizations have currently not implemented these retention requirements and instead tend to retain data indefinitely.

   Suggested approach: Organizations can adopt centralized retention governance, including automated deletion workflows, clearly defined retention schedules and periodic compliance audits. Establishing standardized, legally aligned retention policies — supported by monitoring mechanisms — can enable prompt deletion, reduce compliance risks and strengthen accountability for high-volume digital platforms.

4. **Sector-based view:** Financial services and technology sectors demonstrate advanced and intermediate levels of adoption, whereas sectors such as healthcare, infrastructure and telecom lag, showing basic or unclear maturity levels.

   Suggested approach: This scattered distribution underscores the urgent need for standardized monitoring frameworks to enhance auditability and compliance readiness across sectors.

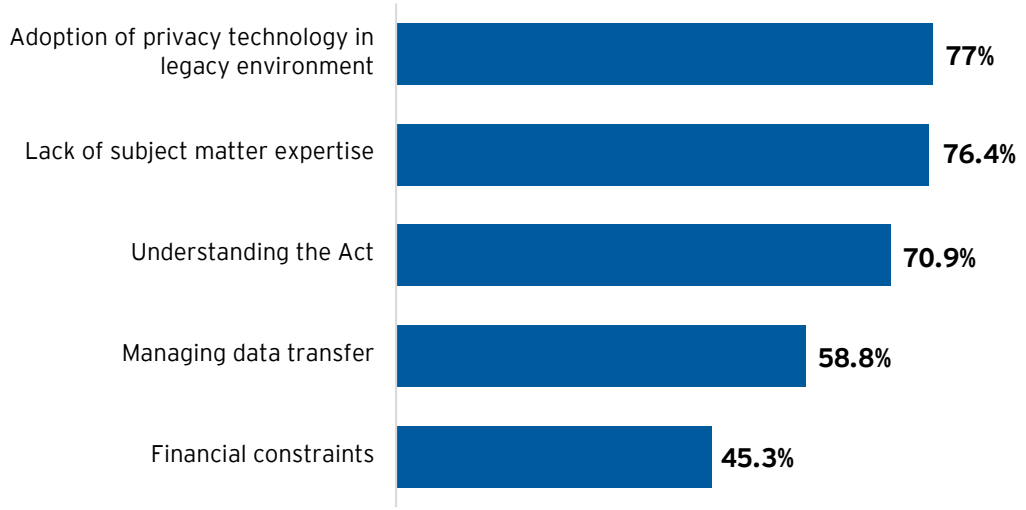
Addressing key challenges that organizations anticipate

The survey highlights several structural and operational challenges as well that organizations expect to encounter as they move toward DPDP compliance. Understanding and interpreting the Act has emerged as one of the key challenges in the survey. Many organizations, especially in sectors such as shipping, metals and mining, education, hospitality and media and entertainment, have indicated low to medium levels of familiarity with the DPDP Act and Rules.

Existing legacy systems pose additional challenge in adoption of tecnological tools. Another challenge that organizations anticipate is lack of insufficient subject matter expertise. Overcoming such challenges is essential for compliance and modern privacy operations.

As companies assess the impact of the DPDP Act and Rules on their business and work through its details, they are also facing challenges related to cross-border data transfers due to varying regulations across regions. At the same time, many organizations are encountering cost and resource constraints while aligning with the DPDP Act and Rules, making compliance more difficult.

Key challenges organizations face in implementing the DPDP Act and Rules



Source: EY Research

A recurring concern across industries is the handling of personal data in an increasingly globalized environment. As organizations map their compliance journeys, many are turning their attention to the implications of cross-border data movement, a critical consideration, especially for multinational operations and digital service providers. The DPDP Act and Rules stance on cross-border data transfers will likely shape how businesses manage customer trust, regulatory risk and operational continuity in the years ahead.

To stay ahead, businesses should consider adopting privacy leading practices, such as implementing robust data transfer agreements, using inter- or intra-group contractual frameworks and evaluating the data protection adequacy of the destination country. These measures can enable lawful and secure data movement while reinforcing long-term compliance and accountability.

As organizations progress towards DPDP Act and Rules compliance, several cross-sectoral challenges are coming into focus.

1. Companies in automobile, manufacturing and education sector highlight insufficient robust technological capabilities required for consent management, automated data discovery, retention governance and rights fulfilment.

2. Insufficient data governance ability impedes the correct interpretation of the Act, with non-expert teams struggling to grasp its technical and legal nuances. Specifically, consumer and financial sectors have experienced trouble in accessing subject matter expertise for data privacy compliance.

3. The lack of sufficient budgetary support and leadership endorsement in seen as an obstruction majorly in sectors like automobile, manufacturing and education.

4. While many organizations prove a conceptual understanding of regulatory obligations, the depth of operational readiness differs significantly across sectors. Specially, infrastructure, real estate, hospitality and shipping have faced trouble in understanding the requirement of the DPDP Act and Rules.

5. Technology, healthcare, financial and consumer sectors express difficulty in managing cross-border data transfers and data localization requirements, largely due to the complexity and global nature of operations.

Strategies to address implementation challenges

Challenges differ meaningfully across organizational levels and roles. To overcome those, organizations can adopt stepwise implementation strategies, which can include:

1. Adopting modular data privacy tools and solutions offered by both local and international vendors. To allow a phased and scalable approach, these tools provide specialized modules for critical compliance needs, such as:

- Identification and documentation of personal data
- Data flow maps
- Universal consent management
- Data Principal rights management

Many solutions also include advanced capabilities like automated data discovery, comprehensive data scanning across enterprise systems and real-time data mapping, enabling more effective identification and management of personal data. Leveraging such tools can ease compliance burdens, especially for organizations with complex data environments or limited internal resources.

2. Conducting organization wide awareness training sessions to build foundational understanding. Collaborating with external specialists to help fill gaps where in-house expertise in privacy is lacking, to enable compliance with legal statutes. This collaboration can also support privacy-related tasks, such as consent management, data identification and mapping and audit preparation.

3. Presenting benchmarking insights and risk-based analyses to leadership to secure budget and executive buy-in.

4. Benchmarking against peers, locally and globally and using industry playbooks to set up clear, practical standards for operational execution. Use phased rollouts and maturity-based roadmaps to bring uniformity across departments or business units.

5. Using modular privacy platforms that map data locations and data flows in real time, which supports better governance of cross-border transfers.

6. Collaborate with external experts to interpret localization requirements and design compliant data transfer mechanisms aligned with operational realities.

7. Migration of legacy systems to modern technology for adoption of privacy technology and data protection measures.

Section 3

How the DPDP Act and Rules impact sectors and enterprises

The DPDP Act and Rules introduces sector-wide implications by reshaping how enterprises collect, process, and manage digital personal data. Across industries, the DPDP Act and Rules influences operational, compliance, and governance practices, requiring enterprises to reassess their data handling frameworks. The DPDP Act and Rules impacts sectors differently, with enterprises expected to align their data practices to regulatory requirements while balancing innovation and growth.

Banking and financial services

The banking and financial sector manages highly sensitive personal and financial data, including account details, transactions and credit histories. Compliance with the DPDP Act and Rules alongside sector-specific regulations, such as those from the RBI and SEBI, often creates regulatory overlaps for institutions operating across banking, securities and investment domains. The key challenge lies in safeguarding personal data while ensuring seamless customer services. In this heavily regulated and risk-sensitive industry, strong data governance, encryption, continuous monitoring, modernization of legacy systems to track historical consent, restructuring of data flows and regular compliance audits are essential to prevent breaches, mitigate fraud risks and maintain client trust.

Impact:

- Need to navigate overlapping mandates between the DPDP Act and sectoral regulations such as those from SEBI and RBI, which increase legal and operational risks
- Re-validation of legacy data based on current consent norms
- Consent-aware system redesign for secure and compliant processing
- Re-validation of data retention schedule to meet data-minimisation expectations without breaching regulatory record-keeping needs
- Heavy dependence on third-party and FinTech ecosystems requires stronger vendor oversight critical for end-to-end compliance

Technology

Tech firms benefit from the Act's flexibility in cross-border data movement, though they also face growing scrutiny of data handling, especially for platforms targetting children. The sector processes large volumes of personal data through platforms, apps, cloud services and digital tools ranging from user identifiers and behavioral data to biometric and location information. Compliance with the DPDP Act and Rules requires tech companies to reengineer systems to support granular consent, transparent data use and secure cross-border data flows. Unlike traditional sectors, the fast-paced nature of tech and its reliance on third-party integrations Application Programming Interfaces (APIs) Software Development Kits (SDKs') and cloud environments make data governance more complex.

Impact:

- Operational ease for global data transfer (subject to restrictions)
- Stricter consent design for child-facing platforms
- Risks around storing personal data offshore without adequate legal safeguards
- Re-architecting platforms to enable granular, real-time consent management
- Stricter governance over third-party integrations and API-based data flows

Healthcare

Hospitals handle extremely sensitive personal data, making compliance with the DPDP Act and Rules essential. The challenge is balancing seamless data sharing among healthcare providers, insurers and patients with strict privacy and consent requirements through secure channels. Therefore, robust governance frameworks are needed to ensure explicit consent and empower patients. Existing regulations like Electronic Health Record (her) Standards and the Clinical Establishments Act provide guidance, however, unclear oversight between the Data Protection Board and the Ministry of Health can lead to fragmented compliance. Additionally, healthcare entities often struggle with fragmented regulatory direction and uneven levels of accountability. Practical challenges include managing patient consent across multiple platforms, ensuring data security amid legacy systems, and aligning internal practices with evolving regulatory expectations. The National Digital Health Mission (NDHM) supports the DPDP Act and Rules by affirming citizens' ownership of their health data. Insights from the U.S. Health Insurance Portability and Accountability Act (HIPAA) emphasize the need for strong compliance systems, which Indian organizations can adopt to meet DPDP standards and adapt to global privacy expectations.

Impact:

- Unclear liability for state-run systems handling personal health data
- Heightened need for data protection in patient records
- Overlaps and conflicts between the DPDP Act and sectoral regulations heighten compliance complexity and regulatory ambiguity

Manufacturing

The manufacturing sector, especially in its digitally transforming state, is increasingly reliant on data from employees, suppliers, IoT-enabled machines and connected production environments. While traditionally not data-intensive from a personal data perspective, the adoption of smart factories, remote monitoring and digital workforce management has significantly increased the handling of personal data. Compliance with the DPDP Act and Rules requires manufacturers to secure personal data across enterprise resource planning (ERP) systems, supply chains and factory automation platforms. Additionally, dealing with third-party vendors, contractors and workforce platforms necessitates strong contractual safeguards and audit trails.

Impact:

- Integration of data protection protocols into industrial and operational systems
- Managing third-party vendor compliance in complex supply chains
- Clear guidelines needed for handling employee data
- Standardized retention of internal and vendor data
- Integration of privacy compliance into shop floor systems

Media and entertainment

The media and entertainment sector handles large volumes of personal data through streaming, subscriptions, digital advertising and audience engagement, including user preferences, viewing history, geolocation and sometimes biometric data. Under the DPDP Act and Rules, companies must ensure transparent data practices, valid consent and secure data sharing with advertisers and partners. Effort is required in balancing hyper-personalized content delivery with compliance, requiring a reassessment of data monetization models and stricter controls across data collection, profiling and cross-platform tracking. Managing consent consistently across devices and formats is now essential to meeting regulatory expectations.

Impact:

- Explicit opt-in for content personalization
- Cross-device data synchronization requires compliant consent capture and usage logs
- Defined data retention periods for analytics
- Transparent consent mechanisms in digital interactions

Auto and mobility

The auto and mobility sector are rapidly transforming through connected vehicles, telematics, ride-sharing and smart mobility services, all generating sensitive personal data such as driver behavior, location, biometrics, infotainment usage and payments. Under the DPDP Act and Rules, companies must ensure transparent consent, secure data handling and accountability across complex digital-physical ecosystems. Efforts are required in embedding privacy controls into systems not originally designed for user consent, while managing data flows across OEMs, suppliers, fleet operators, insurers and tech partners. Updating vehicle systems, apps and backend platforms to support consent tracking, data minimization and real-time controls is now critical for compliance.

Impact:

- Consent-led tracking of location and driver behavior
- Consent frameworks required for in-vehicle data collection and telematics-based tracking
- Secure data sharing is needed between OEMs, mobility providers and third-party tech vendors
- Updates to in-vehicle systems and mobile apps for real-time consent
- Biometrics, if used, must align with consent and retention norms

Consumer, retail and e-commerce

The consumer, retail and e-commerce sectors rely heavily on personal data such as contact details, purchase history, payment information and browsing behavior, to deliver personalized experiences, loyalty programs and targeted marketing and are one of the most impacted sectors. Under the DPDP Act and Rules, businesses must strengthen consent mechanisms, ensure transparent data use and protect consumer data across physical and digital channels. Personalization and privacy need to be balanced, especially amid behavioral targeting and dynamic pricing. Companies must revalidate customer data, secure data sharing with partners and implement integrated governance to manage consent and preferences across websites, apps, stores and supply chains.

Impact:

- Personalization must respect the scope and validity of user consent
- Time-bound retention of payment and fulfillment data
- Third-party vendors (e.g., delivery, payment and analytics) must be contractually compliant
- Omnichannel data flows need unified privacy governance across digital and physical touchpoints
- Real-time opt-out and deletion capabilities expected across e-commerce platforms
- Greater control for users over how their data is profiled and reused
- Need for advanced data management systems to track user activity, manage retention periods, issue timely notifications

Metals, mining and energy

The metals, mining and energy sectors are rapidly digitizing operations through workforce management tools, asset tracking and remote monitoring, leading to the collection of personal data from employees, contractors, visitors and communities, including biometrics, geolocation, health data and IDs. Under the DPDP Act and Rules, these organizations must implement structured consent processes and protect sensitive data across high-risk, distributed environments. With diverse stakeholders, legacy systems and automated systems in play, implementing secure, compliant data handling across the ecosystem is now essential.

Impact:

- Legacy OT systems need updates to support privacy safeguards and access controls
- Structured classification of workforce and surveillance data
- Limited retention aligned with compliance needs
- Consent and access protocols for performance or safety data
- Need for enterprise-wide privacy training to ensure adherence in field operations and remote sites

Telecom

The telecom sector handles vast personal data, including subscriber details, call records, location and internet usage and must comply with the DPDP Act and Rules through strong consent management, data security and transparency. Operators also navigate overlapping regulations like TRAI guidelines and licensing requirements. Upgrading legacy billing and customer systems to track consent, uphold user rights and secure cross-border data flows is essential. Additionally, robust governance is needed to manage third-party partnerships with OTT platforms, data aggregators and service providers.

Impact:

- Compliance with cross-border data transfer mandates
- Need for real-time consent tracking in legacy systems
- Automated consent tracking across systems
- Full lifecycle management of personal data tied to transparency, especially in handling of location, call and internet usage data to protect user privacy
- Investment in data encryption, monitoring and audit capabilities for network and subscriber data

Education

The education sector handles sensitive personal data of students, faculty and staff, including academic records, health details and digital learning behaviors and must comply with the DPDP Act and Rules by implementing strong consent frameworks and data protection across campuses and digital platforms. With growing reliance on online education and EdTech, safeguarding privacy while enabling personalized learning is a key concern. Institutions need to modernize legacy systems for consent management including verifiable parental consent, secure data sharing with third parties and efficiently address data subject rights, while promoting transparency and awareness to build trust and meet regulatory requirements.

Impact:

- Verified parental consent for minors
- Segregated processing of student data
- Managing third-party EdTech vendor compliance and data-sharing agreements
- Updating legacy student information systems for real-time access and correction requests
- Routine audits to ensure child-data handling protocols are followed
- Balancing personalized learning with privacy and regulatory obligations

Hospitality

The hospitality industry processes extensive personal data — from guest IDs and payments to preferences and behavior. Compliance with the DPDP Act and Rules requires hotels and resorts to enforce strict consent management and secure data across all channels, including online bookings, check-ins and loyalty programs. Balancing personalized experiences with privacy obligations, especially as data passes through third parties like travel agencies and payment processors, remains critical. Strong data governance, encryption and regular audits are vital to prevent breaches, reduce risks and protect customer trust in this reputation-driven sector.

Impact:

- Consent-led collection of guest data, especially biometrics
- Opt-out options for profiling or personalization
- Defined retention periods based on service usage

Shipping and logistics

The shipping industry operates within a complex ecosystem involving multiple stakeholders including crew members, port authorities, Customs, logistics providers and customers, each generating vast amounts of personal and operational data. Compliance with the DPDP Act and Rules requires operational efficiency in managing cross-border data flows, maintaining data integrity and securing sensitive information such as crew identities and cargo manifests. Given the international nature of shipping, aligning Indian data protection norms with global standards becomes critical to avoid regulatory friction and maintain seamless operations.

Impact:

- Region-specific compliance for data exchanged during customs processes
- Restrictions on reusing or storing tracking data outside permitted jurisdictions
- Safeguards for handling sensitive logistics and personnel data

Section 4

Impact of DPDP Act and Rules on key stakeholders

The DPDP Act and Rules places defined responsibilities on all stakeholders to ensure personal data is handled lawfully, securely, and transparently. Under the DPDP Act and Rules, stakeholders are required to adopt accountability-driven practices that safeguard individual rights while enabling responsible data processing. The obligations set out under the DPDP Act and Rules establish a shared duty among stakeholders to protect personal data throughout its lifecycle.

Data Fiduciaries: Controllers of personal data

Under the DPDP Act and Rules, Data Fiduciaries, who can be both human entities and organizations, including public entities, are responsible for making decisions regarding lawful, transparent, secure and accountable data handling. The primary responsibility of Data Fiduciaries is to safeguard data through legal and secure processes while providing transparent practices. They are required to uphold data privacy by obtaining valid consent, protecting rights and enabling full lifecycle accountability of processed data.

Key responsibilities:

- The Act permits data processing only with valid consent or when required for the permitted legitimate use by the organization.
- Organizations must provide individuals with clear access to privacy statements that explain their personal data processing practices.
- The purpose of data management must be fulfilled by maintaining accurate and secure information until consent expires or is withdrawn.
- Strong grievance redressal systems must be established with resolution of grievances in defined 90 days window, with special attention to child data protection.

Data fiduciaries responsibilities

Greivance redressal
Establishing effective system for addressing data-related complaints.

Consent and lawful processing
Ensuring data processing aligns with legal and consent requirements.

Data accuracy and security
Maintaining data integrity and security throughout its lifecycle.

Transparent privacy statements
Providing clear and accessible information on data handling practices.

Role of Significant Data Fiduciaries (SDFs)

Certain categories of Data Fiduciaries may be designated as SDF based on factors that increase the impact of their data processing activities. The designation is determined by assessing the volume and sensitivity of the data processed, risks to the rights and freedoms of the Data Principals, impact on the sovereignty and integrity of India and implications for the security of state and public order. Organizations handling large scale or high risk-sensitive data, such as major healthcare providers, banks, fintech companies, e-commerce platforms, technology service providers and large group conglomerates are likely to be classified as SDF. The SDFs are subject to heightened obligations and are required to develop enhanced compliance systems, governance protocols and higher operational resilience.

Additional obligations for SDFs:

- Each organization should appoint one member to serve as Data Protection Officer (DPO), enabling data compliance.
- All organizations must conduct annual Data Protection Impact Assessments (DPIAs) regarding the effects of their data processing operations.
- Data processing entities must undergo external audits to evaluate their data management systems.
- Safeguards related to consent and risk management practices must be established at elevated standards for all entities.
- Data localization for certain personal and traffic data.

Data Processors: Executors of processing activities

Data Processors act on behalf of Data Fiduciaries to carry out personal data processing. While they do not determine the purpose of data used, they must strictly follow the instructions provided by the Data Fiduciary and security clauses mentioned in the contracts. Although the Act does not directly impose obligations on Data Processors, the Data Fiduciaries are responsible for their compliance. Therefore, a strong contractual agreement should be carried out between the parties to ensure compliance.

Importantly, even though Data Processors do not face direct legal consequences under the Act for non-compliance, they may still be held accountable contractually and operationally to multiple Data Fiduciaries. Any failure to follow agreed terms or safeguard obligations could lead to reputational harm, termination of contracts, or loss of business opportunities across several client relationships. Data Processors should proactively establish compliance irrespective of contractual obligations for competitive advantage

Key responsibilities:

- Process personal data only under documented instructions from the Data Fiduciary.
- Implement appropriate security measures to prevent data breaches.
- Promptly report any data breach to the Data Fiduciary.
- Provide reasonable assistance in responding to Data Principal requests, audits and Data Protection Impact Assessments.
- Delete or return personal data after processing is completed.

Data Principals: Owners of personal data

Under the Act, Data Principals are individuals to whom the personal data relates. They are the primary beneficiaries of the rights and protections granted under the Act. Data Principals have the authority to determine how their data is used, shared and retained and organizations processing their data must respect these rights through lawful and transparent practices.
The role of the Data Principal is central to the Act's aim of empowering individuals and ensuring accountability of entities that process personal data. Alongside the rights granted under the Act, certain statutory duties are imposed on the Data Principal to ensure responsible exercise of those rights. Non-compliance with these duties may attract penalties under the Act.

Key responsibilities:

- Follow all applicable laws while exercising their rights under the DPDP Act and Rules.
- Provide only correct and authentic personal data for the intended purpose and avoid impersonating another individual.

- Refrain from withholding or misrepresenting material information when giving personal data for official documents, identification, or proof of address issued by the State or its authorities.
- Avoid submitting false, misleading, or frivolous grievances or complaints to Data Fiduciaries or the Data Protection Board.
- Ensure that information provided during correction or erasure requests is verifiable and authentic.

Consent Manager under DPDP Act and Rules

The DPDP Act and Rules introduces the concept of consent managers, who are independent entities registered with the Data Protection Board of India. These entities serve as intermediaries between Data Principals (individuals) and Data Fiduciaries (organizations processing data), facilitating the management of consent for personal data processing.

Functions and responsibilities

Consent managers must provide platforms that include the following characteristics:

- Enables Data Principals to access and understand the consent procedures in a user-friendly manner
- Allows interoperability with different data fiduciaries, enabling easy management of consents across various services.
- Data Principals should have full authority to approve or disallow specific data processing operations involving personal data.

Regulatory oversight and compliance

Consent managers are required to:

- Maintain a documented system of logs containing detailed records about consents and notices, along with data-sharing transactions, which must remain accessible for a defined period.
- Maintain records for at least seven years, or for longer periods as the Data Principal and Consent Manager may agree upon or as may be required by law.
- Implement protocols to protect against conflicts of interest, preventing relationship conflicts between themselves and data fiduciaries.
- Conduct audits and report technical and organizational control measures to verify DPDP Act and Rules compliance.
- The Consent Manager shall not sub-contract or assign the performance of any of its obligations under the Act and the Rules.
- Ensure that personal data is shared in a way that keeps its content unreadable to them.

Conclusion

The DPDP and Rules Act is reshaping India's data protection landscape, requiring organizations to move beyond compliance toward building lasting trust, accountability and long-term digital resilience. As the regulatory environment evolves, entities must proactively deepen their understanding about the DPDP Act and Rules, and the interplay with the other applicable regulations, including sectoral regulations, strengthen data governance and protection methods and implement robust consent framework. Staying engaged with regulatory developments and fostering a privacy-first culture will be critical to turning challenges into competitive advantages. The time to act is now - organizations that anticipate and adapt will lead India's data protection journey.

Acknowledgements

Thought Leadership authors

- Mini Gupta
- Lalit Kalra
- Priya Badrinarayan Singh

Privacy Core Team

- Murali Rao
- Mini Gupta
- Lalit Kalra
- Sujay Maskara
- Lokesh Jain
- Shruti Shree
- Bhavya Janardhan

Brand, marketing and communications

- Jerin Verghese
- Sharon Dias
- Jatin Rishi
- Kritarth Srivastava

Editorial

- Prosenjit Datta
- Kartik Verma
- Radhika KTP
- Kaveri Nandan
- Shweta Sharma

Design

- Shivam Khanna

Annexure: Glossary of key terms

Terms	Definition
Data Fiduciary	An individual, company, or entity that determines the purpose and means of processing personal data.
Significant Data Fiduciary	A category of data fiduciaries identified based on factors like volume of data processed, sensitivity, or potential impact on national interest.
Consent Manager	A platform or service that enables individuals (Data Principals) to manage their consent preferences for data sharing across services.
Data Principal	The individual to whom the personal data relates.
Data Processor	A person or entity that processes personal data on behalf of a Data Fiduciary by way of a contract.
Personal Data	Any data about an individual who is identifiable by or in relation to such data.
Processing	Any operation performed on personal data, including collection, storage, use, sharing, or erasure.
Purpose Limitation	Principle that data should only be collected and used for the purpose stated at the time of collection.
Data Minimization	Collecting only the data that is necessary for the specified purpose.
Explicit Consent	Clear and informed permission given by an individual before their data is processed.
Breach Notification	The obligation of the Data Fiduciary to report a personal data breach to the Data Protection Board and affected individuals.
Reasonable Safeguards	Technical and organizational measures that ensure data security and protect against breaches or misuse.
Grievance Redressal Mechanism	A system within the organization that allows individuals to raise concerns or complaints regarding their personal data.
Data Localization	The requirement that personal data be stored and processed within the territorial limits of India, or with specific transfer conditions.
Cross-Border Data Transfer	The movement of personal data from India to another country, subject to compliance under the DPDP Act and Rules.

Our offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon Temple
Off SG Highway,
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Gandhinagar
8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International Financial Centre
GIFT City SEZ
Gandhinagar – 382 355, Gujarat
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560 048
Tel: + 91 80 6727 5000

Ecospace
1st Floor, Campus 1C
Ecospace Business Park
Outer Ring Road,
Bellandur - Sarjapura
Area, Varthur Hobli,
Bengaluru Urban – 560103

Bhubaneswar
8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha – 751024
Tel: + 91 674 274 4490

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 700**0**

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

THE SKYVIEW 20
2nd Floor, 201 & 202
Right Wing, Survey No 83/1
Raidurgam, Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur
9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan – 302018

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

6th floor, Sector V,
Building Omega, Bengal Intelligent
Park, Salt Lake Electronics
Complex, Bidhan Nagar
Kolkata - 700 091
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No.301
Building No.1, Mindspace-Gigaplex
IT Park, MIDC, Plot No. IT-5
Airoli Knowledge Park
Airoli West, Navi Mumbai - 400 708
Tel: + 91 22 6192 0003

18th Floor, AltimusPandurang
Budhkar Marg Worli, Mumbai - 400
018 Tel: + 91 22 6192 0503

Pune
C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Pune - 411 045
Tel: + 91 20 4912 6800

Notes

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYIN2601-030
ED None

SK

ey.com/en_in

EY_India EY EY India EY Careers India ey_india