Grant Thornton | 90 in Bharat and beyond

#GTBharat SHAPING VIBRANT INDIA

Digital Personal Data Protection Act and Rules

November 2025

“A contemporary #DataPrivacy regime as a part of India’s #RegulatoryEcosytem, one of the six ecosystems that we are shaping, is critical to help shape #VibrantBharat. The #DPDPA rules represent a significant milestone, balancing two critical priorities- safeguarding individual data rights and fostering responsible business innovation. This is an opportunity for businesses to build trust through responsible data use, advance AI safety and align with global data governance standards.”

Vishesh C. Chandiok

Partner & CEO
Grant Thornton Bharat

Introduction

DPDP Rules 2025: A landmark in India's digital privacy framework

On **13th November 2025,** the Ministry of Electronics & Information Technology (MeitY) notified the long-awaited Digital **Personal Data Protection Act (DPDP Act)** and its detailed **Rules**, marking a historic shift in India's data governance landscape. Through a series of Gazette notifications-**G.S.R. 843(E), 844(E), 845(E),** and **846(E) -** the Government has laid out a **phased enforcement roadmap**: core provisions and the constitution of the **Data Protection Board of India (DPBI)** take effect immediately, consent manager obligations follow **12 months,** and comprehensive compliance duties for organisations become mandatory within **18 months**. The DPBI, headquartered in NCR and comprising four members, will function as a **fully digital adjudicatory authority** with powers to investigate breaches, issue directions, and impose penalties up to INR 250 crore.
The DPDP Rules establish a **robust compliance architecture** built on principles of **consent, transparency, security, and accountability,** redefining how businesses collect, process, and store personal data. Key obligations include **plain-language consent notices, verifiable parental consent for children, breach reporting without undue delay and in a specific format within 72 hours, data retention and erasure norms, and enhanced duties for Significant Data Fiduciaries** such as annual audits and Data Protection Impact Assessments. Cross-border transfers will follow a **"negative list" approach,** allowing flexibility while safeguarding national interests. With these Rules, India moves closer to global benchmarks like the EU's GDPR, compelling organisations across sectors to **embed privacy-by-design,** strengthen governance, and invest in compliance-driven innovation. This is not just a regulatory mandate—it is a strategic imperative to build trust and resilience in the digital economy.

Key highlights of the DPDP Rules 2025

Key stakeholders

- Data principal
- Data fiduciary
- Significant data fiduciary
- Consent manager
- Data protection board of India (DPBI)
- Data processor

Requisite of consent manager

- Must be incorporated in India with = > net worth of INR 2 crores and authorised by the DPBI.
- Acts as data fiduciary
- Implements secure platform for collecting, managing and recording consent.

Rights of data principal

- Access to information
- Erasure of data
- Rectification
- Withdrawal of consent
- Nominate

Significant data fiduciary obligations

- Appoint data protection officer in India
- Annual data protection impact assessment
- Annual audit
- Algorithmic due diligence
- Data localisation requirements

Data breach notification

- Notify each affected data principal and DPBI without delay on becoming aware of breach
- Notify DBPI with detailed breach report within 72 hours in the prescribed manner

Data protection board composition

- Consists of 4 members, commencing the regulatory infrastructure

Seizing the opportunity: Privacy compliance as a strategic advantage

The new rules create a clear opportunity for organisations to strengthen customer trust by demonstrating full compliance with the updated privacy law. Businesses must acknowledge this transformative shift and proactively address the critical implications as they navigate the compliance journey.

Impact

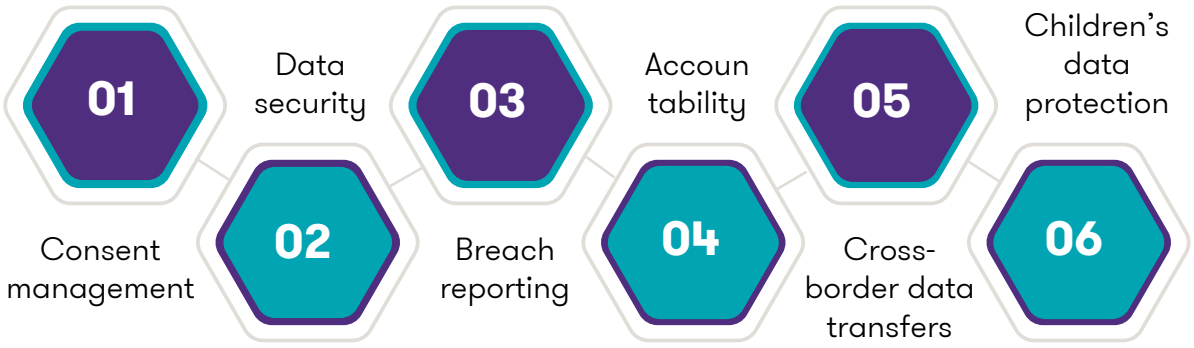
1. Data protection readiness
2. Innovation through compliance
3. Brand reputation, monetary penalties
4. Consent management
5. Transparent communication
6. Global cyber laws compliant
7. Employee training and awareness
8. Data governance and localisation

Opportunity

1. Enhance trust and reputation
2. Competitive edge
3. Global investment attraction
4. Innovation in privacy solutions and tools
5. Privacy centric services
6. Streamlined operations
7. Ethical data monetisation
8. Personalised offerings for customers
9. Improved data governance and insights

Every organisation will follow a distinct data protection trajectory under the DPDP Rules 2025. While some entities already align with global frameworks such as the General Data Protection Regulation (GDPR) and other international standards, the new rules require a fresh evaluation of compliance strategies. Leadership teams must actively assess how existing privacy investments can be optimised to meet DPDP requirements and simultaneously drive operational efficiency and governance excellence.

Key areas to focus (not limited to)



Under the DPDP Rules 2025, implementing strong systems for consent, security, and governance is essential. Organisations now treat compliance as a strategic advantage - aligning with business goals, building trust, and streamlining operations.

Impact on business functions and key initiatives

Key initiatives

Initiative	Data type	Consideration
Payment ecosystem	Payment history, financial information credentials, beneficiary details	Ensure user consent, data retention requirements while complying with data localisation rules
Supply chain	Vendor data, logistics data, product data, inventory supply detail	Transparency and clear-cut data sharing agreements leading to stronger partnerships
External audit and vendor due diligence	Equity holdings, financial statements, intellectual property information	Enhanced assurance, uphold third party accountability and enforce retention policies
Data governance	Access control data, data classification, data cataloguing	Apply strict access controls and categorisation of data to ensure privacy
Mergers and acquisitions	Legal agreements, shareholder data, regulatory compliance records, investee company personal information	Seamless integration and data consolidation ensuring smooth transition
Technology transformation	User engagement metrics, change management data, analytic insights	Higher automation with business logic for faster market turnaround
Consent management	Collection processing use of personal data	Onboarding consent management platforms for exercising rights

Business functions

Function	Data type	Consideration
Cyber	User credentials, logs of security incident data	Strengthen security measures and develop breach identification & notification protocols
Finance and tax	Payroll, financial statements, tax information, payment data	Ensure data localisation, enforce retention policies, and uphold accountability
Information technology	User account, network configuration, incident data, asset logs	Enhanced data handling procedures with stronger systems
Legal and compliance	Third-party contracts, IPR documents, litigation data	Clear accountabilities to be established and ensure continued compliances
Human resources	Job applications, contracts, performance, compensation data	Uphold data principal rights and foster employee training & awareness
Marketing and sales	Customer information, purchase history, prospects and tracking data	Maneuver use of personal data appropriately for targeted marketing
Internal audit	Compliance records, control statements, enterprise risk framework data	Conduct regular privacy audits to ensure adherence to data protection regulations

Sector wise touch points

The DPDP Rules 2025 will impact every sector because all industries handle personal and sensitive data in some form.

01 Financial services

- Customer profiling, authentication, sensitive data
- Process outsourcing - fintech partnerships, data processing, product alliances
- Risk management - credit, AML, fraud, insurance
- Financial information and transaction data
- Fingerprints, facial recognition data for secure access

02 Tech, media, telecommunications and entertainment (TMTE)

- Personal preferences and behaviour
- Device information and location
- Personal data from online activities
- Communication records, media consumption patterns, browsing histories

03 Consumer and retail products

- Name, address and contact numbers
- Consumer preferences
- Payment and transaction data
- Browsing histories, shopping preferences, feedback and reviews
- Service usage, feedback, loyalty programme details

04 Healthcare and life sciences

- Patient health records
- Health insurance
- Clinical trial data
- Biometric and genetic data
- Appointment histories, feedback, health monitoring data
- Diagnostic results, treatment plans, prescription records

05 Tourism and hospitality

- Travel itinerary
- Payment information
- Reservation information
- Guest feedback
- Credit card details, transaction histories, billing information

06 Digital natives

- Identity data - Name, date of birth, gender, profile picture
- Behavioural data- Browsing history, social media likes, comments, and shares
- Health data - Fitness activity, medical history
- Communication data- Chat messages, voice call recordings, emails or feedback submitted via platforms

Draft Rules (3rd January 2025) vs the Final Rules (13th November 2025)

Domain	DPDP Act	Draft DPDP Rule	Final notified DPDPA Rules
Notice (Rule 3)	Notify data principal in English or any of the 22 languages specified in the eighth schedule of the constitution of India about: • Data type • Purpose of processing • Mechanisms to exercise rights • Complaints process	The notice must: • Be clear and understandable • Specify data collected and its purposes • Describe consent withdrawal methods • Describe methods by which rights can be exercised • Describe complaint process method	The notice must: • Clear and understandable independently • Must use clear & plain language • Must include itemised description of personal data and **specify purposes** of processing such personal data • **Give communication link** for data principals to withdraw consent, exercise rights and **make compliant to the board**
Consent manager (Rule 4)	Consent manager shall: • Be registered with the Board • Manage consent on behalf of DP • Comply with prescribed standards	Consent manager must: • Be an Indian-registered company with = > net worth of INR 2 crores • Have operational, technical, and financial readiness • Maintain consent records for 7 years • Avoid conflicts of interest • Ensure secure data sharing	Consent manager must: • Be an Indian-registered company with = > net worth of INR 2 crores • Have operational, technical, and financial readiness • Maintain consent records for 7 years • Avoid conflicts of interest • Ensure secure data sharing
Processing by government entities (Rule 5)	State can process personal data for benefits/services if lawful and as prescribed by the central government	Processing must: • Be lawful and purpose-specific • Be limited to what is necessary • Have reasonable safeguards to prevent breaches	State shall process personal data by following the standards in second schedule with reference to any subsidy, benefit, service, certificate, license or permit • Under law: issued using statutory powers • Under policy: issued via government executive policy • Using public funds: issued through public expenditure

Draft Rules (3rd January 2025) vs the Final Rules (13th November 2025)

Domain	DPDP Act	Draft DPDP Rule	Final notified DPDPA Rules
Rights of data principals (Rule 14)	• Right to access personal data • Right to rectification • Right to erasure • Right to nominate • Right to grievance redressal • Right to withdraw consent	Data fiduciary and consent manager must: • Publish request procedures and identification requirements on their website/app • Enable data principals to request access or erasure of personal data where consent was given • Publish grievance redressal timelines to ensure system effectiveness	Data fiduciary and consent manager must: • Publish request procedures and identification requirements on their website/app • Enable data principals to request access or erasure of personal data where consent was given • Publish grievance redressal timelines to ensure system effectiveness • **Respond to grievances within 90 days**
Data security (Rule 6)	• Ensure personal data protection, even when processing is done by DP • Implement reasonable security measures to prevent breaches	• Use encryption, masking, and virtual tokens • Have access control • Maintain logs to detect and remediate breaches • Ensure data backups • Include security clauses in contracts with processors	• **Include minimum data security measures, such as** encryption, masking, and virtual tokens • Have access control • Maintain logs to detect and remediate breaches • Ensure data backups • Include security clauses, **wherever applicable,** in contracts with processors
Data breach protocol (Rule 7)	Notify the Data Protection Board (DPBI) and affected individuals in case of a breach	• Notify affected individuals **without delay** • Notify DPBI without undue delay • Notify DPBI with breach details and mitigation measures within **72 hours**	• Notify affected individuals **without delay on becoming aware of breach** • Notify DPBI without undue delay **on becoming aware of breach** • Notify DPBI with breach details and mitigation measures within **72 hours.**

Draft Rules (3rd January 2025) vs the Final Rules (13th November 2025)

Domain	DPDP Act	Draft DPDP Rule	Final notified DPDPA Rules
Data retention and deletion (Rule 8)	• Erase personal data upon consent withdrawal or when the purpose is fulfilled. • Ensure Data Processors adhere to retention policies	• Limit data processing to specific purposes • Delete data within 3 years of last interaction (for certain entities) • Notify Data Principals at least 48 hours before deletion	• Limit data processing to specific purposes • Delete data within 3 years of last interaction (for certain entities) • Notify Data Principals at least 48 hours before deletion • Retain personal data, traffic data and logs of processing for a minimum period of one year to fulfill government requests as per seventh schedule
DPO/ Designated person (Rule 9)	• Publish business contact info of the DPO or designated person for handling personal data queries	• Display contact information of the DPO or designated person on the website or app	• Display contact information of the DPO or designated person on the website or app
Processing of child & PWD personal data (Rule 10 and 11)	• Obtain verifiable consent from a parent/guardian • Avoid harmful processing and restrict tracking/advertising	• Adopt technical and organisational measures to ensure verifiable consent • Implement measures for verifiable consent using reliable identity verification, details of identity & age, or via virtual token	• **Clear segregation between rules applicable to processing of personal data of children and persons w disabilities, respectively .** • Adopt technical and organisational measures to ensure verifiable consent • Implement measures for verifiable consent using reliable identity verification, details of identity & age, or via virtual token or authorised entity • Person w disability must be unable to take legally binding decision regardless of adequate support
Transfer of personal data outside India (Rule 15)	• Central Government may restrict data transfer outside India through notifications	• Data fiduciary must comply with requirements specified by the Central Government	• Data fiduciary must comply with requirements specified by the Central Government • All personal data can be transferred subject to restrictions

Draft Rules (3rd January 2025) vs the Final Rules (13th November 2025)

Domain	DPDP Act	Draft DPDP Rule	Final notified DPDPA Rules
Exemption from processing of child personal data (Rule 12)	• Certain class of data fiduciaries or purposes may be exempt from the consent and tracking restrictions, as prescribed	• Certain data fiduciaries are exempt from consent/tracking restrictions for specific purposes like education, healthcare, and safety under prescribed conditions	• Certain data fiduciaries are exempt from consent/tracking restrictions for specific purposes like education, healthcare, and safety under prescribed conditions
Additional obligation for significant data fiduciaries (SDF) (Rule 13)	• Central government may designate SDFs based on factors like data volume and sensitivity • Obligations include DPO and independent auditor appointment, audits, and DPIAs	• SDFs must conduct yearly DPIAs, and audits • Ensure to submit the report to the Board, • Conduct algorithmic due diligence • Follow data localisation for cross-border data transfer	• SDFs must conduct yearly DPIAs, and audits • Ensure to submit the report to the Board, • Conduct algorithmic due diligence to **verify technical measures** • Follow data localisation for cross-border data transfer

Timelines for enforcement of the Act and Rules

Phase I – 13 November 2025 (Notification date)

- All definitions under the Act are finalised.
- The Data Protection Board of India is established with its composition, qualifications, and governance structure defined.
- Chairperson and members of the Board are appointed, along with salary, terms, and conditions for officers and employees.
- A framework for officers and employees is introduced, and provisions for protection under good faith actions are implemented.
- Rule-making powers of the Board come into effect, and amendments to TRAI and IT Act are enforced.

Organisational impact in phase I

- This phase does not impose immediate compliance requirements.
- The regulatory framework begins to take shape, giving organisations time to understand expectations.
- Early readiness planning is advisable to prepare for upcoming compliance obligations.

Phase II – 13 November 2026 (12 months from notification)

- Consent manager registration opens with the Board.
- Technical, operational, and financial conditions for consent managers are published.
- Organisations are permitted to inquire into operational breaches.
- Penalty framework for consent managers is enforced.
- A single point of contact for consent management is introduced, along with interoperable platform requirements.

Organisational impact in phase II

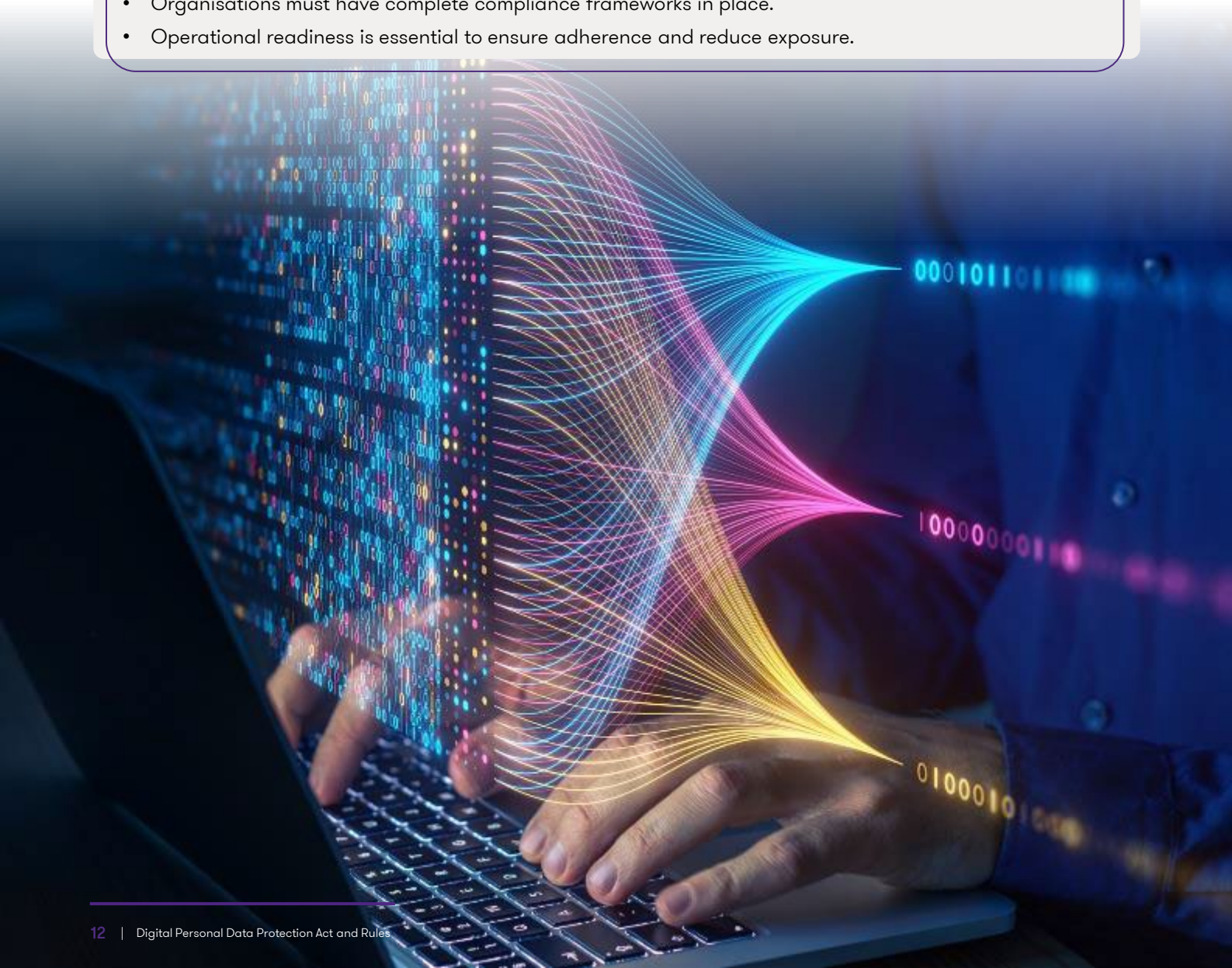
- The consent management infrastructure becomes operationally viable for adoption.
- Organisations begin assessing potential consent management needs.
- Internal processes can be aligned in anticipation of future integration requirements.

Phase III – 13 May 2027 (18 months from notification)

- The complete data protection regime becomes enforceable.
- Terminal application is defined for processing, including legitimate use grounds.
- Consent requirements for data principals are enforced, covering free, specific, informed, and unambiguous consent, along with the right to withdraw consent.
- Data fiduciary obligations such as security and breach notifications are fully implemented.
- Breach detection and response mandates are enforced, along with enhanced protections for children's data.
- Significant data fiduciary obligations are applied.
- India-based Data Protection Officer (DPO) and independent data auditor requirements are enforced.
- Data protection impact assessment becomes mandatory for high-risk processing.
- Cross-border transfer restrictions and Board inquiry powers are implemented.
- Appeals to the Telecom Appellate Tribunal are enabled.
- Penalties for non-compliance are applied, with fines up to INR 250 crore.
- All Act amendments under section 94A are operationalised.

Organisational impact in phase III

- All substantive obligations become fully enforceable in this phase.
- Penalties for non-compliance begin to apply, increasing regulatory risk.
- Organisations must have complete compliance frameworks in place.
- Operational readiness is essential to ensure adherence and reduce exposure.



Compliance roadmap

Conduct a gap analysis immediately

Map current data-processing, consent flows, vendor relationships, logs/audit capabilities against the forthcoming obligations.

Establish governance and appoint roles

With regulatory architecture live, ensure you have oversight, board reporting, internal accountability in place, including the appointment of a DPO where applicable.

Develop or deploy consent management infrastructure

Build or select a system for obtaining, managing, tracking consent and withdrawals, and integrate vendor/processor workflows.

Review and update policies/contracts

Privacy notices, vendor/data-processor contracts, cross-border transfer clauses, data-retention schedules must be updated in line with the Rules.

Build technical/security controls

Logging, monitoring, backup, incident response, breach-notification workflows, data-mapping and inventory.

Communications and awareness campaigns

Educate business units, legal, IT, vendors on upcoming obligations, rights of data principals, internal escalation.

Monitor the timelines

Because obligations will phase-in, align your budget and resourcing with the activation phases—not all obligations apply today, but readiness must start now.

DPBI notifications and advisory

Organisations should keep a close watch on upcoming notifications and advisories that shall be released from time-to-time.

Prepare for enforcement

With the DPBI in place, ensure documentation, audit trails, vendor oversight and internal compliance logs are maintained so you are enforcement-ready.

Our solutions

End-to-end DPDPA compliance support

- DPDPA readiness assessments
- Consent management and notice redesign
- Data inventory and lifecycle management
- Data protection office setup and governance frameworks
- Data breach response preparedness
- Identification and Programme Management Office (PMO) support for integration of privacy enhancing technologies
- Cross-border transfer and vendor-risk reviews
- Data protection impact assessment
- Privacy automation and implementation

Protecting reputation and governance

- Integration of DPDPA compliance into governance practices
- Ensuring airtight compliance to uphold reputation of independent directors

Efficient data management

- Guidance to identify and gather data as per DPDPA requirements
- Streamlining data assimilation and management without manual complexities

Assisting CIOs and CSOs

- Collaborate with our technical experts to align your
- IT systems and security measures with DPDPA requirements

Data protection office setup

- Support in setting up and managing data protection office

Independent data auditor focus

- Fulfilling the need for an independent data auditor as mandated

Expert dispute resolution

- Expert assistance in resolving disputes arising from data breaches

Tailored solutions

- Customised approaches for different industries

“DPDPA is a defining moment in India’s digital journey. When organisations protect personal data with integrity, we don’t just meet regulations; we strengthen citizen trust and help shape a #VibrantBharat.”

Deepankar Sanwalka

Senior Partner
Grant Thornton Bharat

For more information on what these rules and clarifications mean for your business, connect with our experts:

Vishesh C. Chandiok

Chief Executive Officer
Grant Thornton Bharat

E: vishesh.chandiok@in.gt.com

Deepankar Sanwalka

Senior Partner
Grant Thornton Bharat

E: deepankar.sanwalka@in.gt.com

Dinesh Anand

Partner and ESG & Risk Consulting Leader
Grant Thornton Bharat

E: dinesh.anand@in.gt.com

Akshay Garkel

Partner and Cyber Monitoring & Response Leader
Grant Thornton Bharat

E: akshay.garkel@in.gt.com

Jaspreet Singh

Partner and Cyber Assurance & Governance Leader
Grant Thornton Bharat

E: jaspreet.singh2@in.gt.com

Vivek Iyer

Partner and Financial Services Risk Advisory Leader
Grant Thornton Bharat

E: vivek.iyer@in.gt.com

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

● Ahmedabad ● Bengaluru ● Chandigarh ● Chennai ● Dehradun
● Gandhinagar ● Goa ● Gurugram ● Hyderabad ● Indore ● Kochi
● Kolkata ● Mumbai ● New Delhi ● Noida ● Pune

Scan QR code to see our office addresses

www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP
@GrantThorntonBharat
@GrantThornton_Bharat
@GrantThorntonIN
@GrantThorntonBharatLLP
GTBharat@in.gt.com