Grant Thornton

#GTBharat
SHAPING VIBRANT INDIA

A step closer to new privacy laws in India

Draft Digital Personal Data Protection Rules (DPDPR) 2025

February 2025

“A contemporary #DataPrivacy regime as a part of India’s #RegulatoryEcosytem is critical to enable our vision of #VibrantBharat. The proposed #DPDPA rules mark an important step by highlighting the dual priorities of protecting individual data rights and enabling responsible business innovation. At #GrantThorntonBharat, we view this as an opportunity for businesses to build trust, enhance transparency, and align with global data governance standards.”

Vishesh C Chandiok

Partner & CEO
Grant Thornton Bharat

2 Draft Digital Personal Data Protection Rules, 2025

Introduction

In today's era of widespread digital communication, protecting personal information has become paramount. The Digital Personal Data Protection (draft) Rules, 2025, aim to establish a framework that balances individual rights, organisational obligations, and national interests. These Rules apply to organisations managing personal data in India or serving Indian residents and will take effect upon publication, with certain provisions (Rules 3 to 15, 21, and 22) to be notified later.

Formulated after 16 months of expert consultations, the Rules aim to address existing knowledge gaps and provide practical compliance strategies. They clarify business requirements and foster trust within the digital ecosystem by emphasising accountability and transparency through essential provisions such as consent management, processing of children's data, cross-border data transfers, and data breach notifications.

The Rules represent a significant paradigm shift, emphasising stringent data protection and privacy measures that will redefine business operations. Given their sector-agnostic nature, organisations must reinvent and invest strategically to thrive in this new era.

Key highlights

Key stakeholders

- Data principal
- Data fiduciary
- Significant data fiduciary
- Consent manager
- Data protection board
- Data processor

Requisite of Consent Manager

- Needs to be incorporated in India with = > net worth of INR 2 crores and authorised by the DPB.
- 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
- Data Principals to appoint nominees to exercise their rights if they are deceased or incapacitated.
- Portability (case specific)

Significant Data Fiduciary Obligations

- Annual data protection impact assessment
- Annual Audit
- Algorithmic due diligence
- Data localisation requirements

Data Breach Notification

- Notify each affected individual without delay
- Notify Data Protection Board without delay & within 72-hour in the prescribed manner

Penalties: Upto INR 250 crore*

*Draft Rules are currently silent on the Penalty structure

Big shift

This transition offers an opportunity to enhance customer trust through compliance. It is crucial to recognise this significant shift and key implications for organisations as they navigate the journey of compliance.

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

Each organisation's data protection journey is unique, especially those aligned with global privacy laws like GDPR and other global privacy laws. With the draft DPDP Rules 2025, leadership teams will likely leverage existing privacy compliance investments to enhance operational efficiency.

Key areas to focus (not limited to):

01 Consent management
02 Data security
03 Breach reporting
03 Accountability
05 Cross-border data transfers
06 Children's data protection

Implementing robust systems for these areas will be crucial. Organisations will see compliance as a strategic opportunity to align with business objectives, improve trust, and enhance existing functions.

4 Draft Digital Personal Data Protection Rules, 2025

Impact on business functions and key initiatives

Business functions

Function	Data type	Consideration
Cyber	User Credentials, logs of security incident data	Strengthen security measures and develop breach 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	Secure informed consent, uphold data principal rights and foster employee training & awareness
Marketing and sales	Customer information, purchase history, prospects and tracking data	Maneuver use of PII 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

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 information	Onboarding consent management platforms for exercising rights

*Business functions and key initiatives are illustrative and may vary based on the specific line of business and sector of operation

Sector wise touch points

The Draft Rules are set to have a widespread impact across various sectors, given that nearly every sector, in one way or the other, handle personal and sensitive data.

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

Healthcare and Lifesciences

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

Tech, Media, Telecom and Entertainment (TMTE)

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

Tourism and Hospitality

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

Consumer, Retail & E-commerce

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

Digital Natives

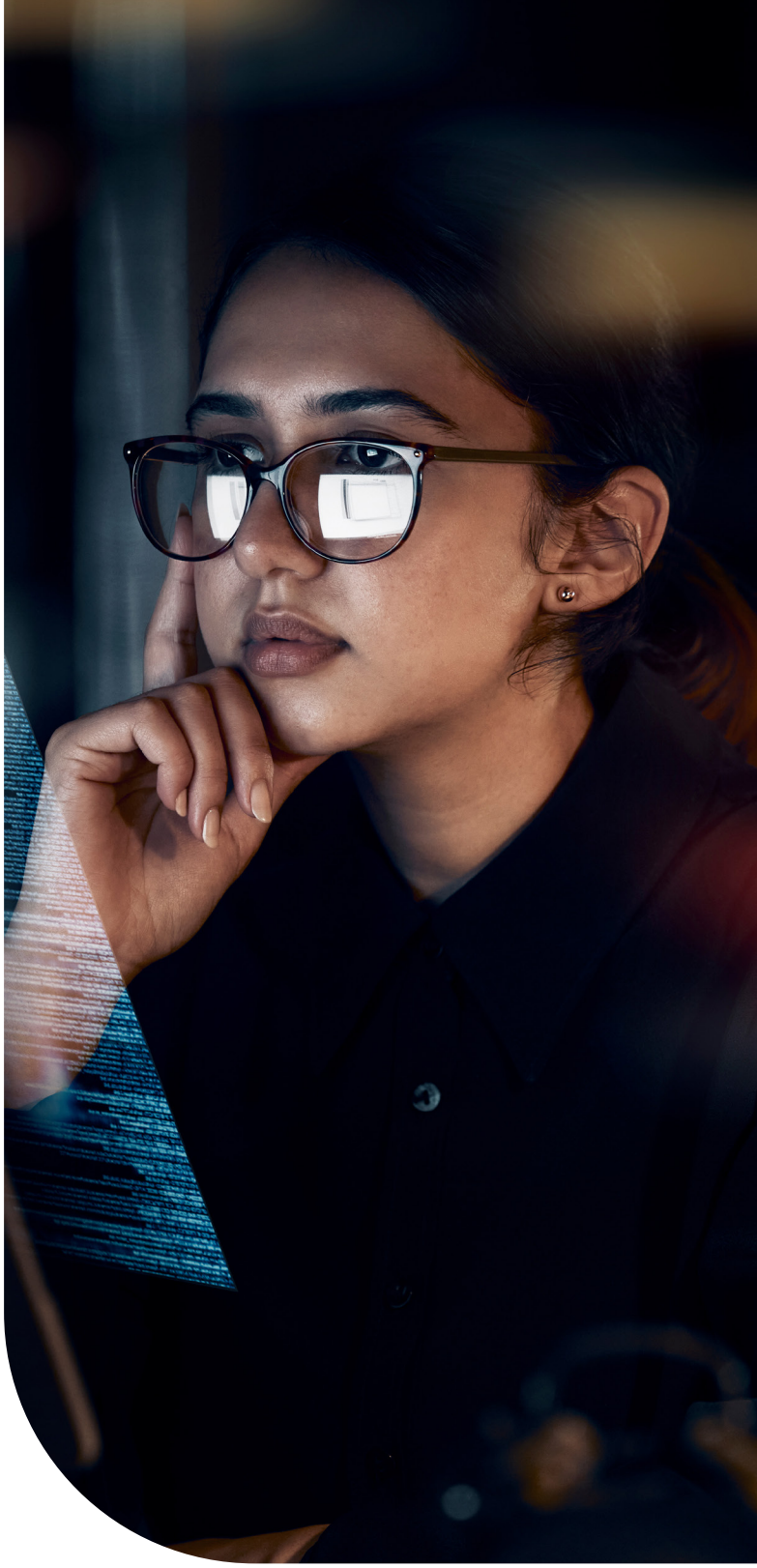
- Identity data: Name, date of birth, gender, profile picture
- Behavioural Data: Browsing history, Social media likes, comments, and shares
- Health data: Fitness activity, Medical history
- Communication data: Chat messages, Voice call recordings, emails or feedback submitted via platforms

Timelines

01	**Intimation of personal data breach to Data Principal** **Intimation of personal data breach to Data Protection Board** **Notify Data Protection Board in the prescribed manner**	Immediate (without delay) Immediate (without delay) Within 72 hours
02	**Retention of logs and personal data**	1 year
03	**Erasure of personal data of Data Principals in the event of 3 years of inactivity. Applicable only to fiduciaries viz. e-commerce, gaming and social media intermediaries**	48 hours of intimation to Data Principal prior to erasure of personal data
04	**Maintenance of consent records by Consent Manager**	7 years
05	**Significant Data Fiduciaries to conduct Data Privacy Impact Assessments and Audit**	Annually

Adoption roadmap

1. **Gap analysis**
   (1-3 months)
2. **Implementation**
   (3-6 months)
3. **Deploy automation tools**
   (3-6 months)
4. **Readiness checks**
   (5-6 months)
5. **Independent audit**
   (6-9 months)
6. **Relevant declarations**
   (9-12 months)
7. **Ongoing sustenance**
   (Annual)



Some organisations, in anticipation of the new regulations, have already embarked upon**

- A gap analysis exercise to identify areas needing improvement
- Readiness checks, particularly for those categorised as Significant Data Fiduciaries, to ensure they are prepared to meet the stringent requirements of the Rules

**Indicative of what GT has observed in the market, this may not be a representative sample for all organisations

Our solutions

Compliance assessment

- Comprehensive compliance assessment for adherence to data protection regulations.
- Project Management Office for seamless implementation and compliance.

Assisting CIOs and CSOs

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

Tailored solutions

- Customised approach for different industries

Data Protection Office setup

- Support in setting up and managing Data Protection Office

Efficient data management

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

Independent data auditor focus

- Fulfilling the need for an independent data auditor as mandated

Protecting reputation and governance

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

Expert dispute resolution

- Expert assistance in resolving disputes arising from data breaches

Data breach response

- First response
- Data breach root cause analysis and investigation
- Breach management PMO

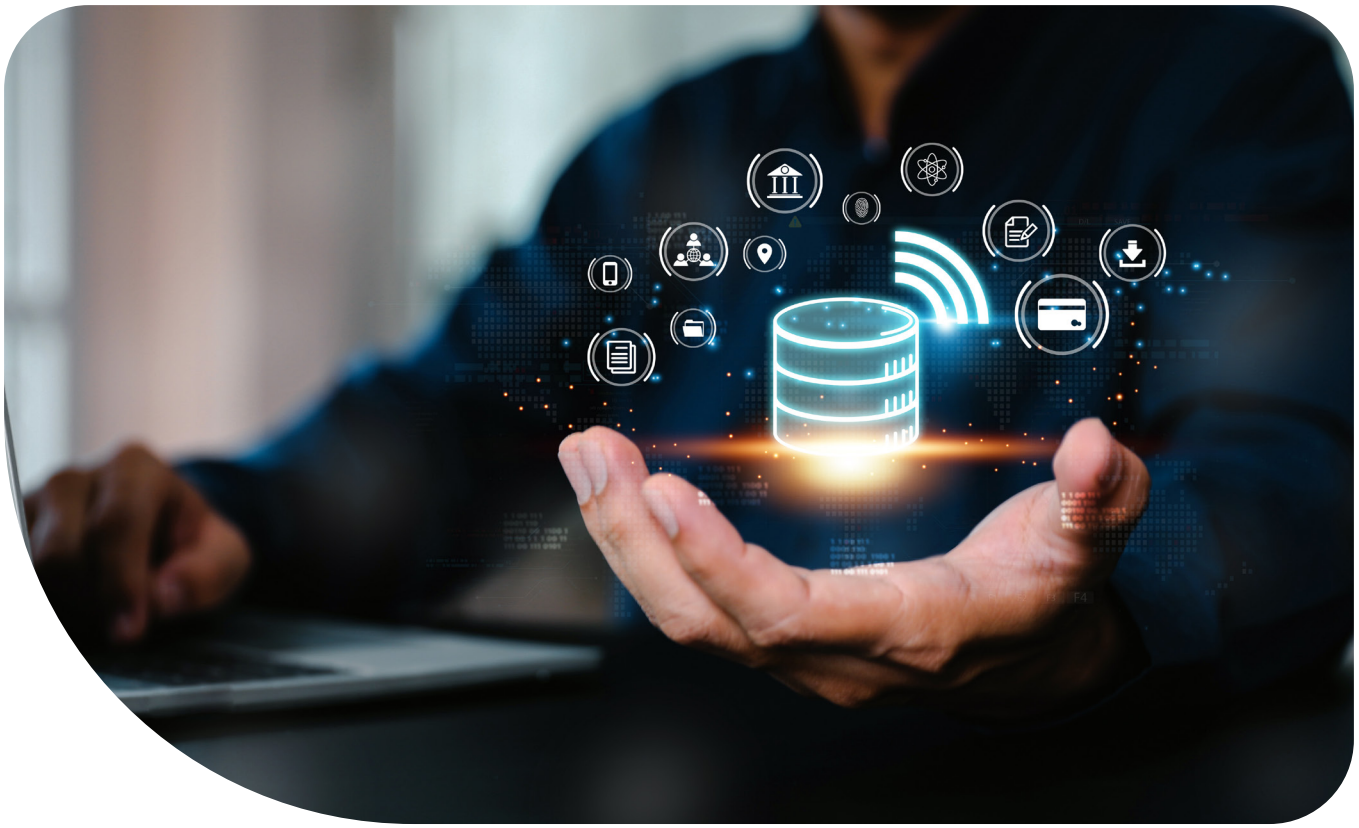
Consent management

- Consent management platforms audit
- Consent management framework advisory

> The draft DPDPA Rules, 2025 is an excellent opportunity for businesses to create an ecosystem that enables customer trust. This will undoubtedly reform the country's data protection landscape and prepare us to create a digital-first #VibrantBharat.

Deepankar Sanwalka

Senior Partner
Grant Thornton Bharat



For more details on what the Draft Rules & Act means for your organisation, please contact:

Gaganpreet Singh Puri
Partner, ESG & Risk Consulting
Grant Thornton Bharat
E: gagan.puri@in.gt.com

Akshay Garkel
Partner, Cyber & IT Risk
Grant Thornton Bharat
E: akshay.garkel@in.gt.com

Jaspreet Singh
Partner, Cyber & IT Risk
Grant Thornton Bharat
E: jaspreet.singh2@in.gt.com

Scan the QR code for more details on DPDPA, 2023 and How GT Bharat can help

Disclaimer: This document reflects GT's unique perspective. Stay tuned for more updates and content as we continue to engage with the government, ministries, peers, and public consultations to gain further clarity. While some points may still need additional discussion, we encourage companies to start evaluating their next steps to ensure compliance with the DPDP Act and Rules. We're here to help you navigate this journey with confidence and ease!

Annexure: Overview of the draft DPDPA Rules 2025

The Ministry of Electronics and Information Technology (MeitY) has introduced the **Digital Personal Data Protection Rules, 2025**, (3rd Jan 2025) as subordinate legislation to offer essential details and an implementation framework for the Digital Personal Data Protection Act, 2023 (11 Aug 2023). It is open for consultation till 18 February 2025

Key provisions

Rule 3 – Notice	The notice must be clear and independently understandable, detailing personal data collected and its purposes.
Rule 4 - Consent Managers	Consent Managers are entities that enable secure and transparent consent management, meeting technical, financial, and operational criteria.
Rule 5 – Processing by Government	Government entities permitted to process personal data for public services like subsidies, benefits, and certifications, provided they adhere to the standards prescribed under second schedule
Rule 6 – Reasonable security safeguards	Data Fiduciaries are required to implement robust security measures such as encryption, access controls, and monitoring systems to prevent data breaches.
Rule 7 – Breach Notification	In the event of a breach, fiduciaries must promptly notify affected individuals and the Data Protection Board within 72 hours, detailing the nature of the breach, mitigation measures, and safety precautions.
Rule 8 – Data retention & deletion	Data Fiduciaries must erase personal data as specified in the Third Schedule if it falls under the categories prescribed therein.
Rule 9 – Contact Information	Data Fiduciaries must publish the contact details of the Data Protection Officer or privacy representative prominently on their website or app.
Rule 10 & 11 – Child data processing	The rules mandate verifiable parental consent for processing child' data, with limited exemptions for educational institutions, healthcare providers, and safety-related entities under strict conditions.
Rule 12 – Significant Data Fiduciaries	The rules mandate additional obligation for Significant data fiduciaries such as annual DPIA & audit, algorithmic verification, cross border data restriction
Rule 13 – Data Subject Rights	The rules grant individuals rights to access and correct their personal data, right of grievance redressal and right to nominate
Rule 14 – Cross border data transfer	The central government will set requirements for transferring personal data outside India, and only Data Fiduciaries meeting these criteria will be allowed to do so.
Rule 15 – Exemption for research purposes	Provision of DPDPA shall not be applicable on processing of personal data for research, archiving or statistical purposes
Rule 16 to 22 – Board establishment	The rules define board composition, appointment process, salary, service conditions, meeting procedures, and guidelines for digital office functioning and staff appointments.

Schedule

Schedule 1 – (Rule 4)	Conditions of registration and obligation of consent manager
Schedule 2 – (Rule 5(2) & 15)	Standards for processing of personal data by State and processing for research, archiving and statistical purpose
Schedule 3 - Rule 8(1)	Classes of data fiduciaries and their timeline for retention of personal data
Schedule 4 – Rule 11	Classes of data fiduciaries on whom rule 10 is not applicable under strict conditions
Schedule 5 – Rule 16 to 20	Terms and conditions of service of Chairperson and other Members
Schedule 6 – Rule 16 to 20	Terms and conditions of appointment and service of officers and employees of Board
Schedule 7 – Rule 22	Central Government may call for information from data fiduciaries as specified

For more information: https://www.meity.gov.in/writereaddata/files/259889.pdf

Great Place To Work® Certified DEC 2024-DEC 2025 INDIA ™

Best Workplaces™ in Professional Services Great Place To Work® INDIA 2024

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 • 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

10307 | RD | JA