tsaaro consulting®

2025

# WHITEPAPER

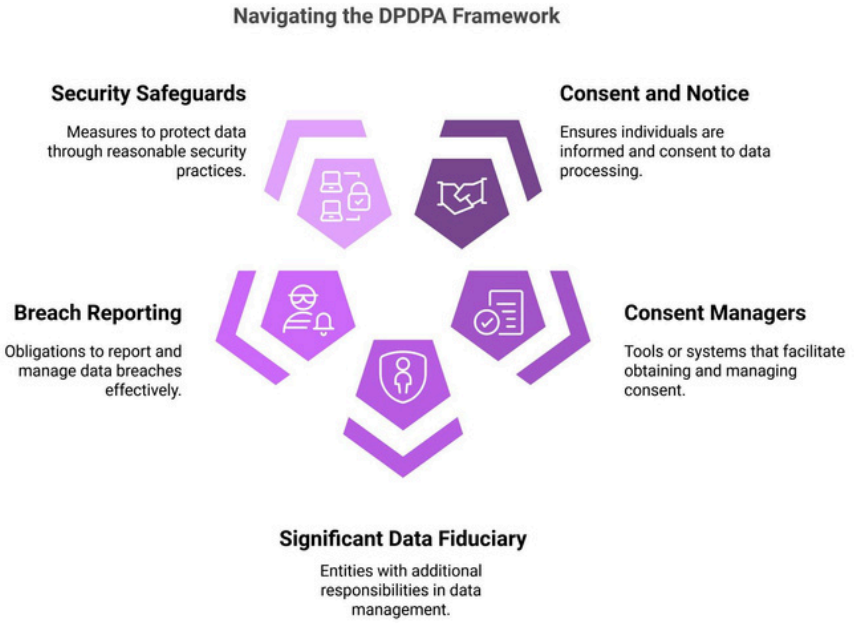
JANUARY- 2025

## Draft DPDP Rules 2025:

Implementation Guide

# OVERVIEW

India is on the cusp of a transformative shift in data protection, as the Digital Personal Data Protection Act, 2023 (**'DPDPA'**) prepares to reshape the landscape of digital privacy. The release of the draft Digital Personal Data Protection Rules, 2025 (**'Draft DPDP Rules'**) marks a pivotal moment in this process, offering essential guidance on the implementation of the DPDPA.




By exploring the critical intersections between the Act and the Rules, the whitepaper provides a deep dive into how these legal instruments collectively aim to fortify privacy and data protection in India's increasingly digital landscape. It provides a **practical implementation roadmap**, guiding organizations on how to comply with the DPDPA and the Draft DPDP Rules, through a structured approach from conducting data protection impact assessments to establishing governance frameworks.

Ultimately, the whitepaper aims to support organizations in meeting their legal obligations while contributing to India's broader vision of a secure and privacy-respecting digital ecosystem.

# FOREWORD

**Akarsh Singh A.**
***(CEO & Founder, Tsaaro Consulting)***

The introduction of DPDPA marks a transformative shift in India's approach to data privacy, reshaping how personal data is collected, processed, and protected. Amid technological advancements and growing concerns over privacy, the DPDPA aims to safeguard individual rights while giving people more control over their data. The newly notified Draft DPDP Rules clarify the Act's practical application, providing essential guidance on compliance and enforcement.

In the evolving landscape, automation plays a crucial role in ensuring compliance with the DPDPA, given the complexity of data management. It streamlines tasks like consent management, data access requests, breach notifications, and audits, enabling real-time, scalable compliance. Beyond regulatory adherence, the DPDPA emphasizes embedding privacy by design into daily operations, fostering a culture of privacy hygiene.

***Top 3 Key Insights: Hot-Takes Worth Considering:***

1. A robust consent mechanism is essential for explicit, informed consent during data collection and processing.
2. Data mapping ensures transparency throughout the data lifecycle, from collection to disposal.
3. Organizations must maintain up-to-date policies and legal agreements, including necessary data protection clauses, to safeguard stakeholders.

By focusing on these pillars, organizations can build a solid foundation for responsible data management under the DPDPA.

# TABLE OF CONTENTS

# INTRODUCTION

On **January 3, 2025**, the *Ministry of Electronics and Information Technology (MeitY)* unveiled the highly anticipated draft of the **Digital Personal Data Protection Rules, 2025** (Draft DPDP Rules) for public consultation. In 2023, after several iterations of bills, India enacted its foremost Digital Personal Data Protection Act, 2023 (DPDPA). The DPDPA, designed to safeguard individual's privacy and protect personal data in India's digital landscape, received presidential assent on August 11, 2023. However, its operationalization has been delayed due to the absence of the corresponding administrative rules.

### *Public Consultation*

The Draft DPDP Rules, 2025 are now open for public consultation, with stakeholders invited to submit their feedback through the **MyGov Portal** until **February 18, 2025**. This 45-day consultation window provides a valuable opportunity for businesses, industry groups, legal experts, and other stakeholders to engage with the proposed provisions and offer insights that could shape the final version of the rules.

### *Implementation Timeline*

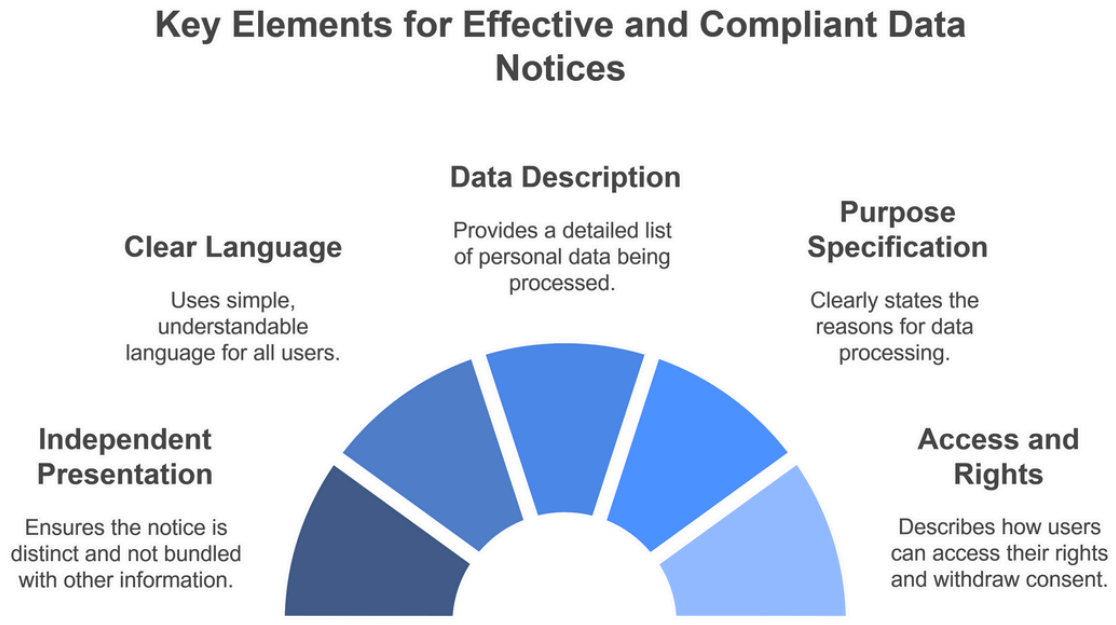
Provisions on the **Data Protection Board** (Rules 16-20) will take effect upon notification, while key operational requirements (Rules 3-15, 21, and 22) will follow later without a set timeline. This phased approach aims to give businesses time to adapt, though clearer timelines are needed for effective preparation.

# REQUIREMENT OF CONSENT AND NOTICE

Central to the Act is the principle that personal data can only be processed in accordance with the provisions of DPDPA and for a lawful purpose, for which data principal has given its explicit consent. Thus, 'consent' emerges as pivotal to processing operations.

Under the DPDPA, personal data can only be processed for a lawful purpose with explicit consent from the **Data Principal**. Consent should be **free, specific, informed, unconditional, and unambiguous** as per **Section 6(1)** of the Act. **Section 4(1)** mandates Data Fiduciaries to process data only with explicit consent, aligning with global privacy standards. **Section 5** requires a notice detailing the data being processed and its purpose.

The Draft DPDP Rules, under **Rule 3,** specifies rigorous criteria for consent notices aimed at ensuring informed and specific consent. This notice must adhere to specific requirements to guarantee clarity and accessibility for the Data Principal.



## *Implications for Organizations: Ensuring Compliance and Transparency*

To meet the requirements of the **DPDPA** and **Draft DPDP Rules**, organizations must ensure the following:

1. **Clear and Understandable Notices:**

Notices should be clear, concise, and easily understandable and should-

- Itemize the personal data being collected.
- Specify the purposes for processing the data.
- Detail any associated services linked to the data processing.
- Explain how data principals can exercise their rights

2. **Cookie Consent for Online Platforms:**

Websites and online platforms that use cookies to collect, store, or process personal data must:

- Obtain explicit consent from data principals before using cookies.
- Provide a cookie consent notice that clearly explains:
  a. The types of cookies used.
  b. The purpose of the cookies.
  c. How the data will be used.

3. **Privacy Notice and Consent Management Strategy:**

- Implement an **effective privacy notice** that clearly communicates data collection practices and the purposes behind them.
- Develop a user-friendly consent management system, enabling data principals to provide and withdraw consent with ease.

4. **Handling Data Principal Requests:**

- Organizations must have processes in place for handling Data Principal Requests, such as allowing data principals to acess their data, rectify any inaccuracies and erase their data, in line with the rights provided under the DPDPA.

## *Scope for Clarity*

The Draft DPDP Rules do not provide clarity on how notice requirements should be handled for legacy customers - those who may have provided consent prior to the implementation of DPDPA. This lack of specification could lead to inconsistencies in how organizations communicate consent information to individuals.

# CONSENT MANAGERS AND THEIR ROLE

The unique concept of the **Consent Manager**, introduced by the DPDPA, distinguishes it from other global privacy laws. **Section 2 (g) of the DPDPA** defines "Consent Manager" as a person registered with the Data Protection Board (**'Board'**), who acts as an intermediary to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

**Rule 4** of the **Draft DPDP Rules**, along with the **First Schedule**, outlines the registration process and obligations of a Consent Manager.

## *Registration Requirements for Consent Managers*

The **First Schedule, Part A** of the **Draft DPDP Rules 2025** outlines the following conditions for registering a Consent Manager:

1. **Company Incorporation**: The applicant must be a company incorporated in India.
2. **Capacity to Fulfill Obligations**: The company must demonstrate adequate technical, operational, and financial capacity to meet its responsibilities as a Consent Manager.
3. **Financial Health**: The company must have sound financial health and a reputable management team.
4. **Net Worth**: The company should have a net worth of at least ₹2 crore.
5. **Business Potential**: The applicant must show adequate business potential, strong capital structure, and favorable earning prospects.
6. **Reputation of Leadership**: The company's directors, Key Managerial Personnel (KMP), and senior management must have a reputation for fairness and integrity.
7. **Corporate Governance**: The company's Memorandum and Articles of Association must include provisions ensuring adherence to obligations such as avoiding conflicts of interest with Data Fiduciaries. Any amendments require prior Board approval.
8. **Alignment with Data Principal Interests:** The company's operations should be aligned with the interests of Data Principals.

**9. Independent Certification:** Certification must confirm that:

- The platform facilitates Data Principals to give, manage, review, and withdraw consent in line with data protection standards.
- Technical and organizational measures are in place to comply with the standards and obligations set by the Board.

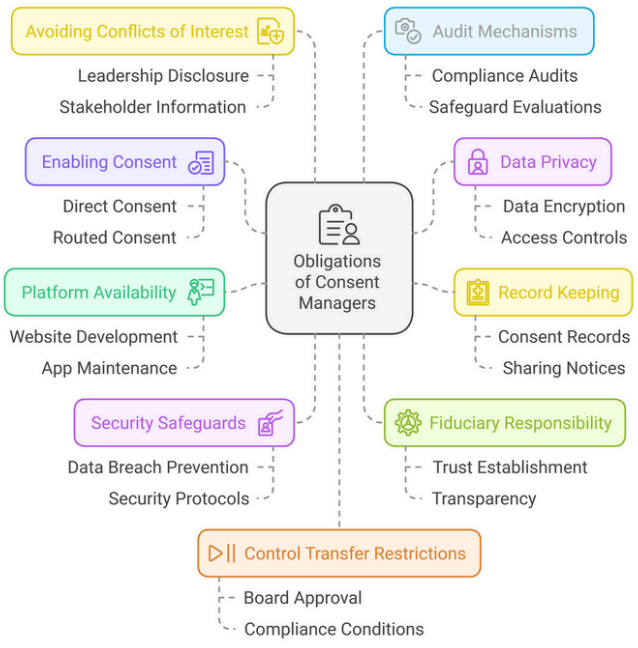
Additionally, **Part B, Item 11** specifies that the Consent Manager must publish information about:

- The company's leadership, including promoters, directors, Key Managerial Personnel, and senior management.
- Individuals holding over 2% of the company's shares.
- Corporate entities where the company's leadership holds over 2% equity.
- Any other information as required by the Board to ensure transparency.

Before applying to the Data Protection Board of India (Board), applicants must meet specific conditions listed in Part A of the Schedule, submitting the required documents as per the Board's guidelines. The Board will review the application and may conduct an inquiry to confirm compliance. If satisfied, the applicant will be registered with their details published; if not, the application is rejected with reasons provided.

## *Obligations of Consent Managers*

**Part B** of the **First Schedule** outlines the key obligations of Consent Managers.



# PROTOCOLS SURROUNDING PERSONAL DATA BREACH

**Rule 7** establishes a framework for how Data Fiduciaries must handle breaches once they are aware of them, mandating intimation to affected Data Principals and the Board.

### *Notification to Data Principals (Rule 7(1))*

When a Data Fiduciary becomes aware of a personal data breach, it must inform each affected Data Principal in the following manner-

1. T**imeliness:** The breach must be reported "without delay".
2. **Clarity and Conciseness**: The notification must be written in a clear, concise, and plain language to ensure Data Principals understand the breach and its potential impacts.
3. **Details to Include:** The notification must cover several specific details about the breach:

- **Description of the breach:** This includes information on the nature, extent, timing, and location of the breach.
- **Consequences of the breach:** Data Principals should be made aware of the potential risks they face due to the breach.
- **Mitigation measures:** The notification must include what measures the Data Fiduciary has implemented or is implementing to mitigate the breach's impact.
- **Safety measures for Data Principals:** It should outline what actions the Data Principal can take to protect themselves from harm.
- **Contact information:** The Data Fiduciary must provide contact details for someone who can respond to inquiries about the breach.

### *Notification to the Board (Rule 7(2))*

Data Fiduciaries are also required to report the breach to the Board.

**Initial Notification (Without Delay)**

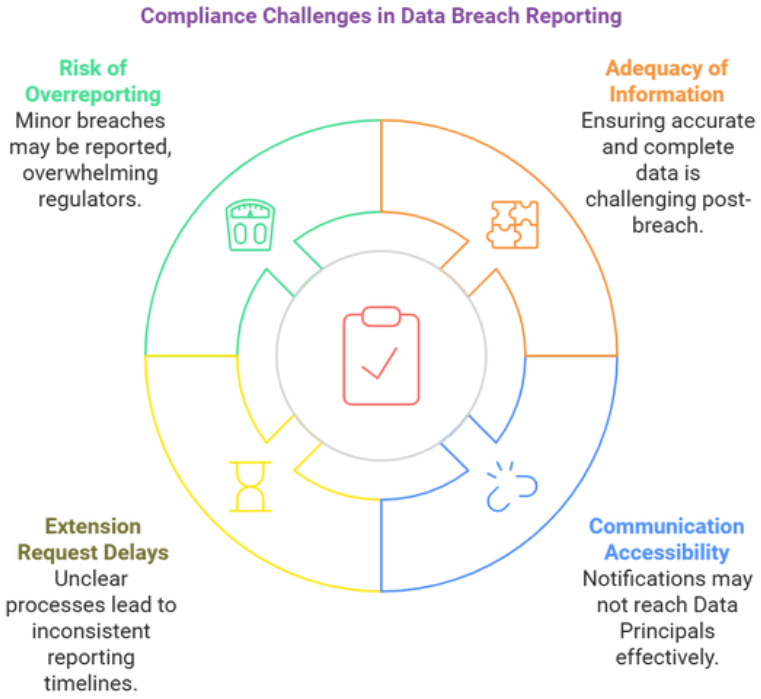
- The Data Fiduciary must immediately inform the Board of the breach, including basic information like the nature, extent, timing, location, and likely impact of the breach.

- This initial notification should be as comprehensive as possible, even if the breach's full scope is not yet clear.

**Detailed Report (Within 72 hours):**

**Within 72 hours** of becoming aware of the breach (or a longer period upon request to the Board), the Data Fiduciary must submit an **updated and detailed report**. This report must include:

- **Detailed description** of the breach (expanding on the initial information).
- **Circumstances leading to the breach**: Including causes and factors that contributed to the breach.
- **Mitigation measures:** Detailed actions taken or proposed to reduce the breach's impact.
- **Remediation efforts**: Any steps taken to prevent a recurrence of the breach.
- **Findings about the breach's origin**: This may include details about the individuals or entities responsible for the breach (if known).
- **Report of notifications to Data Principals**: A summary of the notifications sent to affected Data Principals.



## *Strategic Recommendations for Businesses*

1. Establish a Robust and Flexible Incident Response Plan
   - **Triage and Documentation**: Implement a triage system for rapid breach classification and detailed, real-time documentation.
   - **Roles & Responsibility Clarity**: Assign specific roles to legal, IT, and communications teams to avoid delays during breach response.
   - **Breach Simulations**: Conduct periodic breach simulations to validate plan effectiveness.

2. Develop Customizable Breach Notification Templates
   - **Tailored Templates**: Create templates for various breach types (data loss, unauthorized access, etc.) and audience (Data Principals, Board).
   - **Clear, Actionable Information**: Provide Data Principals with clear guidance on steps to protect their data and contact information for inquiries.

3. Implement Cross-Departmental Collaboration and Staff Training
   - **Cross-Departmental Breach Response Team (BRT):** Form a team with members from IT, legal, and compliance to streamline breach management.
   - **Ongoing Training:** Conduct regular training on Rule 7's requirements and breach communication protocols.

4. Strengthen Data Security Infrastructure
   - **Data Minimization & Segmentation:** Only collect necessary data and implement segmentation to reduce breach impact.
   - **Real-Time Monitoring & Encryption:** Invest in anomaly detection tools, encryption, and data masking to prevent breaches.
   - **Automated Detection Tools:** Utilize AI-based tools for early breach detection.

## *Scope for Clarity*

*Both the DPDP Rules and the CERT-In Directions have specific timelines for reporting personal data breaches and security incidents, respectively. However, the lack of clarity or harmonization between these timelines creates confusion for organizations attempting to comply with both sets of regulations.*

# VERIFIABLE CONSENT MECHANISMS

**Rule 10** focuses on ensuring transparency, accountability, and privacy rights for vulnerable populations by addressing the need for verifiable consent in processing personal data of children and persons with disabilities who are represented by lawful guardians.


### *Technical and Organizational Measures for Verifiable Consent*

1. **Identity Verification Mechanisms:** Data Fiduciaries must ensure that the individual providing consent as a parent or guardian is an adult, and identifiable as required by law. Verification Methods may include-

- **Details of Identity and Age:** The Data Fiduciary can rely on available identity details, ensuring they meet the legal standards for verification.
- **Voluntary Details and Virtual Tokens:** Where the parent or guardian provides voluntary identity and age details, these must be mapped to a verifiable token issued by a legally designated authority (e.g., Central Government, State Government, or a designated entity). This includes details verified by a Digital Locker service provider.

2. **Due Diligence in Consent Collection:**

- **Reliability and Authenticity:** The due diligence process involves ensuring that the person consenting is not only an adult but is legally recognized as the parent or guardian under applicable laws.

- **Verification of Guardians:** For persons with disabilities, it is critical to verify that the guardian is appointed by a recognized authority.

### *Challenges: Verification Complexity and Technological Barriers*

While the use of tokens and services like Digital Locker allows for interoperability between governmental systems and the private sector, ensuring that consents are legitimate and verifiable, however, it is significant to note that not all parents or guardians may have access to the necessary verification tools (e.g., Digital Locker). The implementation of alternative methods for verification may be required, especially for rural or underserved populations.

### *Strategic Recommendations for Businesses*

1. **Investment in Technology:** Organizations should invest in state-of-the-art verification technologies and ensure compliance with the rules through seamless integration with government-issued services like Digital Locker.
2. **Public Awareness Campaigns:** Conduct campaigns to inform parents and guardians about the consent process and how their data is being protected.
3. **Cross-Agency Collaboration**: Facilitate collaboration between government agencies and private entities to ensure a cohesive and user-friendly consent verification process.

Beyond legal compliance, Rule 10 reflects an ethical commitment to protect vulnerable individuals and prevent exploitation, aligning with data fiduciaries' corporate social responsibility (CSR) goals.

# COMPLIANCE AND CHALLENGES FOR SIGNIFICANT DATA FIDUCIARIES

As concerns surrounding data privacy and protection continue to rise, entities managing substantial volumes of personal data play an increasingly critical role. Certain entities are to be designated as Significant Data Fiduciaries (SDF) under the DPDPA due to the scale of data they process and the potential risks they pose to individual privacy.

An SDF represents a sub-category of Data Fiduciaries that manage large volumes of personal data or process sensitive data with heightened risks to individual rights and freedoms. **Section 10** of DPDPA empowers the Central Government to notify any Data Fiduciary as a SDF on the basis of criteria laid down thereunder-

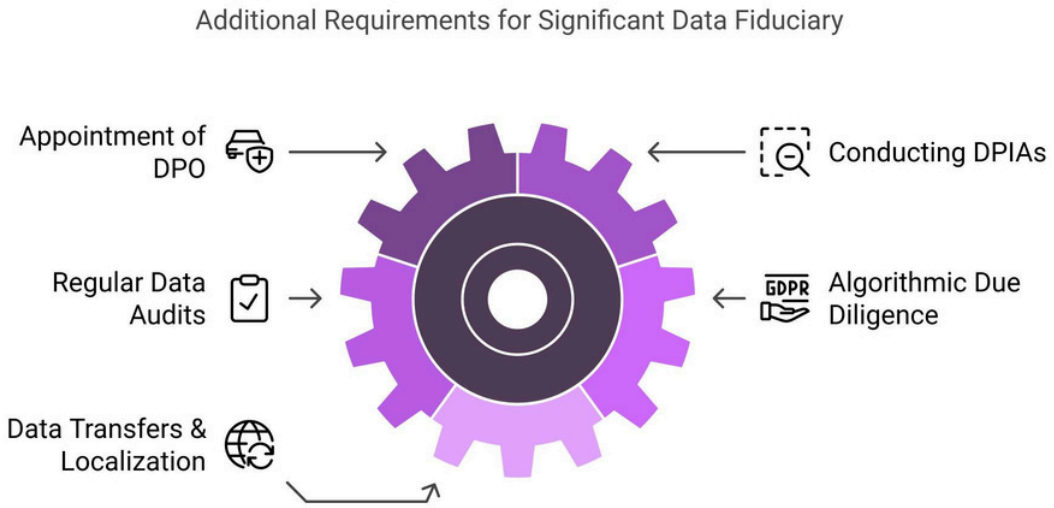
- **Data Volume and Sensitivity**: Entities processing significant amounts of personal or highly sensitive data, such as financial, health, or biometric information, are primary candidates for SDF classification. **For example**: A large bank which holds extensive financial data, including account details and transaction records for millions of customers.

- **Potential Risks to Individuals:** Businesses that expose Data Principals to considerable risks, such as unauthorized access, data breaches, or misuse, may also qualify as SDFs. **For example:** An insurance company processing detailed personal data, including policyholder medical histories, claims records, and family health information.

- I**mpact on National Interests:** Organizations whose data processing activities could influence critical areas such as public order, national security, or electoral integrity may face stricter oversight and classification as SDFs. **For example:** A major telecommunications provider handling extensive communication data, including call records, internet usage, and geolocation data, plays a critical role in national infrastructure.

### *Additional Obligations of SDFs under DPDPA & Draft DPDP Rules*

The DPDPA and Draft DPDP Rules provide for certain additional obligations of SDFs. Non-compliance with these obligations can result in penalties of up to INR 150 crores for each instance of a breach. Additional compliances for SDFs include-




According to the Draft DPDP Rules, SDFs are required to conduct Data Privacy Impact Assessments (DPIAs) and audits at least once every **twelve months**, establishing an annual compliance obligation. Furthermore, SDFs are required to furnish to the Board a Report containing significant observations in the DPIA and audit.

### *Strategic Recommendations for Businesses:*

Although the timeline for central government to notify SDFs remains unclear, organizations, especially large entities handling sensitive data, should proactively begin preparing for the additional obligations that may arise. Sectors such as **banking, healthcare, e-commerce, telecommunications, and social media platforms,** which process large volumes of personal or sensitive data, must begin considering the implications of DPDPA and the Draft DPDP Rules.

# CROSS BORDER DATA TRANSFERS

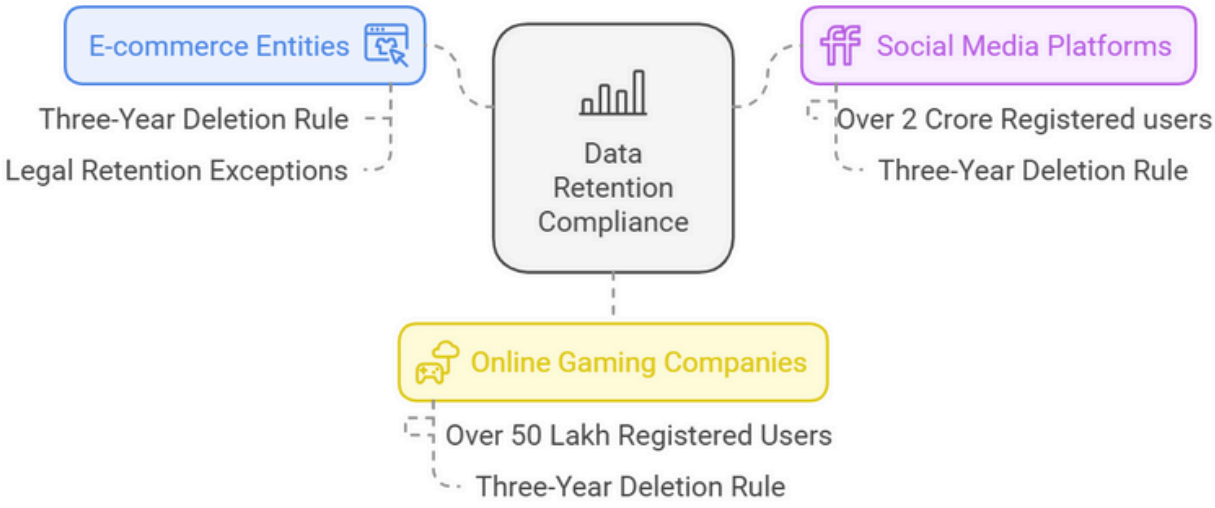
**Section 16** of the DPDPA allows the transfer of personal data to any territory, except those designated as "blacklist" countries by the central government. The DPDPA does not mandate specific transfer mechanisms but remains subject to existing Indian laws that impose stricter data protection and localization requirements in sectors like banking, finance, insurance, telecommunications, and investments. These laws will continue to apply alongside the DPDPA.

While DPDPA adopts a blacklist approach, the Draft DPDP Rules, as per **Rule 14** enables the Central Government to impose further data localization requirements as necessary, ensuring sector-specific compliance and enhanced protection.

# DATA RETENTION PRACTICES

Data retention refers to the practice of storing collected data for a defined period or until the purpose for which it was collected is fulfilled. The principle of storage limitation requires organizations to retain data only for as long as necessary to fulfill its intended purpose. Once this purpose is achieved, the data should be securely deleted. However, if legal obligations require the data to be retained or archived, organizations must comply with those requirements while ensuring secure storage.

The Draft DPDP Rules introduce specific data retention timelines for certain industries. Additionally, it requires the Data Fiduciary to notify Data Principals **at least 48 hours prior to data deletion**, providing them an opportunity to take action if they wish to retain their data.



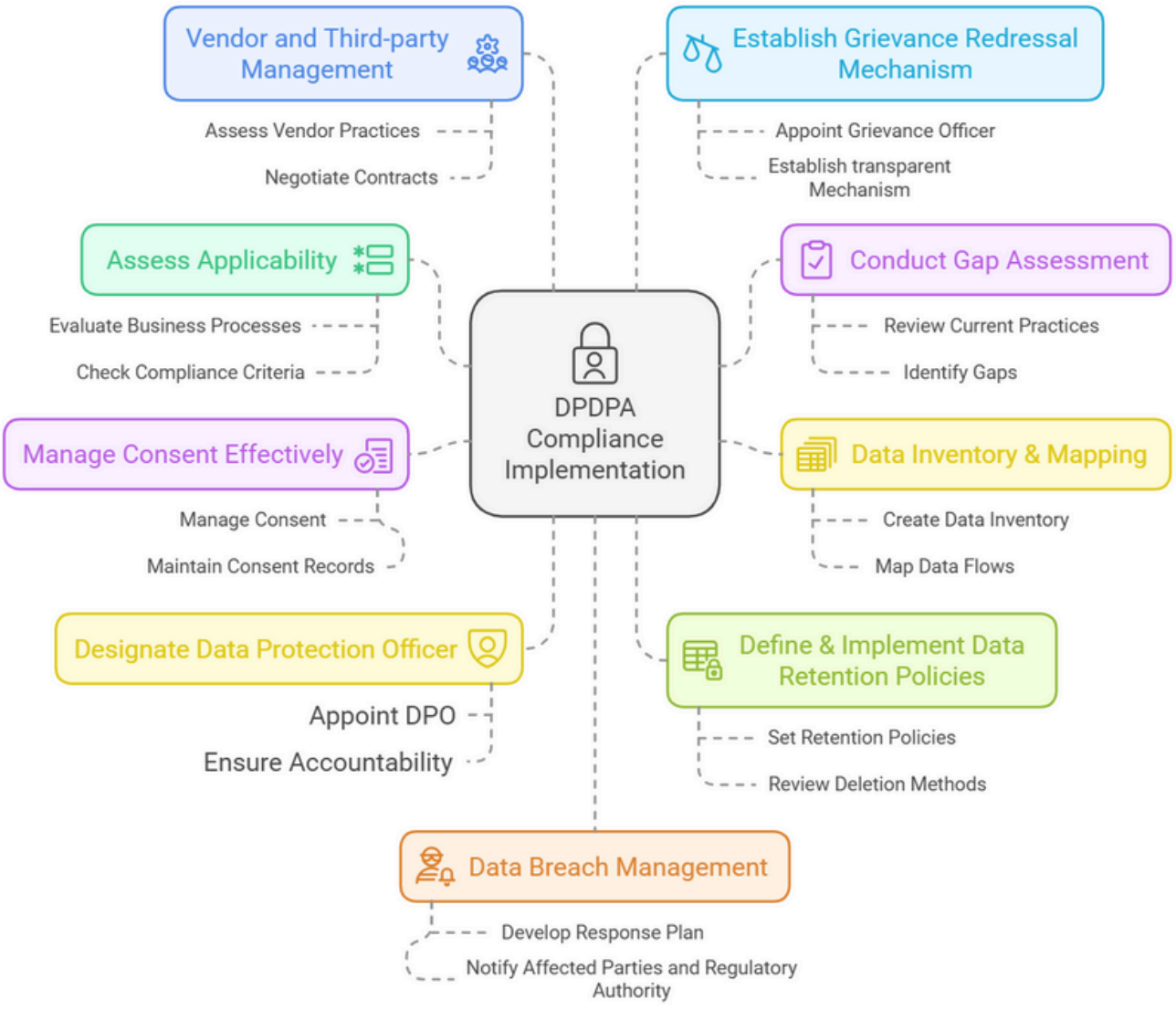
# NAVIGATING TECHNICAL & ORGANIZATIONAL MEASURES

Implementing appropriate technical and organizational measures is crucial for protecting personal data and ensuring compliance with data protection regulations. **Section 8 (4) of DPDPA** requires a Data Fiduciary to implement appropriate technical and organizational measures to ensure effective compliance with the law and rules made thereunder. The Draft DPDP Rules outline the minimum requirements for reasonable security safeguards, including the following-

- **Securing Personal Data: Implement reasonable security measures to prevent data breaches, including encryption, obfuscation, masking, or virtual tokenization.**
- **Access Control: Control access to computer resources used by the Data Fiduciary or Data Processor.**
- **Monitoring & Logging Data: Maintain visibility into data access with logs, monitoring, and reviews to detect and address unauthorized access.**
- **Continuity: Ensure continued data processing in case of data loss or compromise through measures like data backups.**
- **Data Retention: Retain logs and personal data for at least one year, unless required otherwise by law, for breach detection, investigation, and remediation.**
- **Processor Contracts: Include provisions in contracts with Data Processors to enforce security safeguards.**
- **Compliance Measures: Implement both technical and organizational measures to ensure compliance with security protocols.**

# IMPLEMENTATION ROADMAP FOR COMPYING WITH DPDPA AND THE RULES

To ensure compliance with DPDPA, organizations must follow a structured approach. The following steps outline a comprehensive roadmap for organizations to adhere to the DPDPA and Draft DPDP Rules and safeguard personal data-



# KEY TAKEAWAYS

| Rule No. | Domain | Summary |
|---|---|---|
| **Rule 3** | **Notice Framework** | 1. Businesses must provide clear notices to users about how their personal data will be used.<br>2. The notice should specify the data types, purposes, and related services or benefits.<br>3. It must include a link to the company's website, explain how to withdraw consent, and detail how to exercise rights or file complaints with the DPB. |
| **Rule 4 and First Schedule** | **Consent Manager** | 1. Consent Managers allow users to give, manage, review, and withdraw consent for data processing.<br>2. They must be registered with the Data Protection Board and meet specific conditions and obligations.<br>3. Consent Managers must operate independently and avoid conflicts of interest with Data Fiduciaries. |
| **Rule 5 and Second Schedule** | **Government Organizations processing Personal Data** | 1. Government organizations can process personal data for subsidies, services, and permits, ensuring legality, necessity, security, and data accuracy, while informing individuals about its use.<br>2. Individuals must consent to receive benefits, or the benefit must be authorized by law or public funding provisions. |
| **Rule 6** | **Reasonable Security Safeguards** | 1. Data Fiduciaries must implement security measures like encryption, access controls, and monitoring to protect personal data.<br>2. These measures should ensure data confidentiality, integrity, availability, and include breach detection and incident response.<br>3. Contracts with Data Processors must require security measures that meet technical and organizational standards to prevent data breaches. |

| Rule No. | Domain | Summary |
|---|---|---|
| **Rule 7** | **Intimation of Personal Data Breach** | 1. Data Fiduciaries must notify affected individuals and the Board immediately after a data breach.<br>2. Within 72 hours, they must provide detailed breach information, including timing, impact, and containment efforts.<br>3. Notifications to affected individuals must be included in the report to the Board for transparency and accountability. |
| **Rule 8 and Third Schedule** | **Data Retention** | 1. Personal data must be retained for a maximum of three years, starting from the later of the Data Principal's last request or the commencement of the Draft Rules.<br>2. SDFs like gaming, social media, and e-commerce must delete data after three years, except for account maintenance or token-based services.<br>3. SDFs must notify data principals 48 hours before erasing data; retention is allowed only for legal compliance.<br>4. Other Data Fiduciaries must independently determine when data no longer serves its purpose and set a retention timeline. |
| **Rule 10, 11 and Fourth Schedule** | **Children Data and Persons with Disabilities** | 1. Data Fiduciaries must obtain verifiable consent from a parent or guardian before processing data of children or persons with disabilities, using appropriate measures.<br>2. Organizations must confirm that the consenting parent is an identifiable adult.<br>3. The relationship between the child and parent does not need verification, but for persons with disabilities, the guardian must be legally appointed.<br>4. Certain entities like healthcare, education, and childcare providers are exempt from specific requirements regarding children's data. |
| **Rule 12** | **Obligations of SDFs** | 1. SDFs must conduct annual DPIAs and audits by an independent auditor, submitting a report on the findings.<br>2. SDFs must ensure that algorithmic software used for personal data is designed and verified to protect data principal rights. |

| Rule No. | Domain | Summary |
|---|---|---|
| **Rule 12(4) r/w Rule 14** | **International Data Transfer (Scope for Sectoral Data Localisation)** | 1. The Government may set conditions that Data Fiduciaries must follow before sharing or transferring personal data.<br>2. The Government can recommend that SDFs keep personal and traffic data within India.<br>3. Sectoral data localization requirements, like those in the financial sector (RBI guidelines), may apply. |
| **Rule 13** | **Data Principal Rights** | 1. Data Fiduciaries and Consent Managers must publish details on how Data Principals can exercise their rights on their website or app.<br>2. They must specify response times for addressing grievances and implement necessary measures to ensure timely resolution. |
| **Rule 5(2) r/w Rule 15 and Second Schedule** | **Exemption for research, archiving and statistical purposes** | 1. Exemptions from certain DPDPA provisions apply for research, archiving, and statistical purposes with appropriate safeguards.<br>2. These safeguards must ensure lawful processing, data minimization, accuracy, limited retention, security, and accountability. |
| **Rule 16-20** | **Data Protection Board** | 1. Aggrieved parties can submit digital appeals to the Appellate Tribunal, paying fees through digital systems, with potential fee waivers.<br>2. The Tribunal operates digitally, follows natural justice principles, and can set its own procedures and summon individuals. |
| **Rule 21** | **Appeal** | 1. Aggrieved parties can file digital appeals with the Appellate Tribunal, along with a fee.<br>2. The Tribunal operates digitally, follows natural justice, and can regulate its procedures and summon individuals. |
| **Rule 22 r/w Section 36 DPDPA and Schedule 7** | **Calling for Information from Data Fiduciary or Intermediary** | 1. Disclosure of information may be restricted if it threatens India's sovereignty or security, unless prior written permission is granted.<br>2. The government can request data for national security, legal compliance, or to assess Data Fiduciaries, as per Section 36 of the DPDPA. |

# CONCLUSION

In conclusion, as India approaches a transformative shift in data protection with the introduction of the DPDPA and the release of the Draft DPDP Rules, organizations must act swiftly to ensure compliance. The DPDPA establishes a comprehensive framework for personal data protection, and the Draft DPDP Rules provide essential guidance for its implementation. Together, these legal instruments shape the future of digital privacy in India, making it crucial for businesses to align their data handling practices with the soon-to-be-operational Indian law on data protection.

By following the practical roadmap outlined in this whitepaper, organizations can address key compliance requirements, from consent management to data breach reporting, and navigate the complexities of data protection with confidence. This strategic approach will not only help organizations meet their legal obligations but also contribute to building a secure, transparent, and privacy-respecting digital ecosystem in India.

### *Key Contributors:*


- **Akarsh Singh A** (CEO & Founder,Tsaaro Consulting)
  Contact: +91 7543898606, akarsh@tsaaro.com
- **Krishna Srivastava** (Co-Founder & Director, Tsaaro Consulting)
  Contact: +91 7760923421, krishna@tsaaro.com
- **Bhaskara Nand Shukla** (Director, Tsaaro Consulting)
  Contact: +91 9119999054, bhaskara@tsaaro.com
- **Mahima Sharma** (Senior Data Protection Consultant, Tsaaro Consulting)
- **Arohi Pathak** (Senior Data Protection Consultant, Tsaaro Consulting)
- **Manika Sharma** (Senior Data Protection Consultant, Tsaaro Consulting)
- **Zoya Shabbir** (Data Protection Consultant, Tsaaro Consulting)
- **Janvhi Rastogi** (Data Protection Consultant, Tsaaro Consulting)


### *References:*


1. *The Draft Digital Personal Data Protection Rules, 2025.*
2. *The Digital Personal Data Protection Act, 2023.*
3. *The General Data Protection Regulation, 2016 (Regulation (EU) 2016/679).*
4. *The Information Technology Act, 2000.*
5. *Computer Emergency Response Team (CERT-In) Directions, accessible at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf*
6. *The Ministry of Electronics and Information Technology (MEITy), Explanatory Note to Digital Personal Data Protection Rules, 2025, accessible at: https://www.meity.gov.in/writereaddata/files/Explanatory-Note-DPDP-Rules-2025.pdf*

# Our Services

tsaaro consulting

## DATA PRIVACY

- ✓ Regulatory Gap Assessment (GDPR, DPDPA, CCPA/ CPRA and 50 others)
- ✓ Privacy Program Implementation
- ✓ Privacy by Design Assessment
- ✓ Privacy Automation Platform Implementation
- ✓ Industry Standards Implementation (ISO 27701:2019, NIST PMF, AICPA PMM, SOC 2 Type 2 Privacy)
- ✓ DPO as a Service
- ✓ EU-Rep as a Service
- ✓ Privacy Risk Assessment and Remediation

## GRC

- ✓ Industry Standards Implementation (ISO 27001:2022, NIST CSF, NIST SP 800-53, SOC 2 Type 2, HIPAA)
- ✓ GRC Platform Implementation
- ✓ Cyber Risk Quantification (FAIR Assessment)
- ✓ Cyber Maturity Assessment
- ✓ Cloud Security Assessment (ISO 27017/18)
- ✓ Data Governance
- ✓ Third-Party Risk Management
- ✓ Consent Management

## SYSTEM INTEGRATORS

We are the **resellers** of the mentioned tools & help with efficient **implementation** of the same via expert **staff augmentation**.

- ✓ Securiti.ai
- ✓ Skyflow
- ✓ OneTrust
- ✓ Privado
- ✓ BigID
- ✓ Scrut
- ✓ Exterro
- ✓ Automation
- ✓ Secuvy.ai
- ✓ Vanta

## TECHNICAL SECURITY

- ✓ Vulnerability Assessment & Penetration Testing
- ✓ Red/ Purple/ Blue Teaming
- ✓ Threat Intelligence
- ✓ MDR/ XDR/ MSSP services

## AI COMPLIANCE

- ✓ EU AI Act Compliance
- ✓ Ethical Impact Assessment


Website
**www.tsaaro.com**

Email
**info@tsaaro.com**

## OFFICE ADDRESS

### AMSTERDAM
Regus Schiphol Rijk, Beech Avenue 54-62, Het Poortgebouw, 1119 PW, Amsterdam, Netherlands.
Phone: +31-686053719

### DELHI NCR
ATS Bouquet, Tower C, Office No. 302, Sector - 132, Noida, Uttar Pradesh - 201304, India.
Phone: +91 9557722103

### BENGALURU
Manyata Embassy Business Park, Ground Floor, E1 Block, Beech Building, Outer Ring Road, Bengaluru - 560045, India.
Phone: +91 9557722103

### MUMBAI
Supreme Business Park, Unit No. B-501, 5th Floor, Wing 'B', Powai, Mumbai, Maharashtra, 400076, India.
Phone: +91 9557722103

### PUNE
Tech Centre, 5th Floor Rajiv Gandhi Infotech Park, MIDC, Hinjewadi Pune, Maharashtra, 411057, India.
Phone: +91 9557722103