BHARAT GAIN
Bharat Growth And Inclusion Network

# Draft Digital Personal Data Protection Rules 2025

**A Detailed Look at Each Stakeholder Group and How They Will Be Affected by the Draft Digital Personal Data Protection Rules, 2025**

# Draft Digital Personal Data Protection Rules 2025

*A Detailed Look at Each Stakeholder Group and How They Will Be Affected by the Draft Digital Personal Data Protection Rules, 2025*

As part of the broader movement toward a data protection and privacy-secure internet, the Ministry of Electronics and Information Technology (MeitY) enacted the Digital Personal Data Protection Act (DPDPA) in August 2023. Building on this, MeitY has now released the Draft Digital Personal Data Protection Rules, 2025 (DPDP Rules, 2025), which elaborate on the Act's provisions and provide detailed instructions for their implementation.

The provisions concerning the Data Protection Board (Rules 16-20) will take effect once they are officially published in the gazette. On the other hand, key operational requirements detailed in Rules 3-15, 21, and 22 will be enforced at a later date, although no specific timeline has been provided for their implementation. This phased implementation may allow industry players, including emerging start-ups and MSMEs, the required time to transition and adapt to the new rules.

A wide range of stakeholders will be impacted by the new rules, with some new entities emerging as a result of the legislation. Let's examine how each of these stakeholders is affected, what their responsibilities are under the rules, and the potential implications for them with the Digital Personal Data Protection Rules, 2025.

# DATA FUDICIARIES (DFs)

**Entities Affected:** Companies, organizations, and individuals who process personal data (e.g., businesses, e-commerce platforms, tech companies).

Key Obligations under the rules

- Companies must explain clearly to users what data they are collecting, why, and how it will be used. Users should also be able to withdraw consent easily or file complaints. (Rule 3)
- Companies must implement strong security practices such as encryption and access control to protect personal data and maintain logs for data protection. (Rule 6)
- In case of a data breach, companies must inform users and the Data Protection Board (DPB), detailing the breach's impact, actions taken, and prevention measures. The initial notification to DPB should happen within 72 hours. (Rule 7)
- Companies are required to inform users at least 48 hours before deleting their personal data, unless the user logs into their account, contacts the company for the specified purpose, or exercises their rights regarding the data processing. (Rule 8)
- Rules set a maximum data retention period of three years for DFs, suc e-commerce entities (with two crore or more registered users), online gaming intermediaries (with fifty lakh or more registered users), and social media intermediaries (with two crore or more registered users). (Rule 8)

- Companies must provide contact details of their Data Protection Officer or the responsible person on their website or app for user inquiries. (Rule 9)
- Companies must offer ways for users to file complaints related to their data processing. (Rule 13)
- The transfer of personal data by DFs outside India is restricted and must follow conditions set by the Central Government, as and when they get notified. If data is processed in India, it cannot be transferred abroad without meeting these conditions. The same rules apply if data is processed outside India for offering goods or services to individuals in India. (Rule 14)
- Parental consent is required for collecting data from children, with some exceptions for services like healthcare or education. (Rules 10 & 11)

## Our Take

The rules impose significant obligations on Data Fiduciaries, which may be seen as an additional compliance burden. However, they also establish important security standards, moving beyond potentially restrictive and outdated measures. The data retention rule, which applies only to certain classes of Data Fiduciaries, introduces some uncertainty, and further clarification may be needed on the rationale behind this distinction. The rules require prompt breach notifications to data principals and the board, but the absence of a clear threshold for notifications may result in DFs reporting minor incidents, potentially overburdening regulatory bodies and complicating the notification process. Platforms also need to put in place systems to verify the parent's identity—either using existing information, new details, or third-party government services.

# SIGNIFICANT DATA FIDUCIARIES


According to the DPDP Act, the Central Government can designate you as a Significant Data Fiduciary (SDF) based on factors such as the volume and sensitivity of the data you handle, and the risks posed to data principals' rights, state security, democracy, and public order.

- An officer designated by the Secretary of MeitY may carry out the assessment to notify you or your class as an SDF (Seventh Schedule). As an SDF, you have additional obligations:
- You must conduct a Data Protection Impact Assessment and an audit every 12 months to ensure compliance with the Act and rules.
- The results of the Data Protection Impact Assessment and audit must be documented, and a report containing significant observations must be submitted to the Data Protection Board.
- You must ensure that your algorithmic software used for processing personal data does not pose risks to the rights of data principals. (Rule 12)
- Based on recommendations from a committee as and when appointed by the Central Government, you must ensure that certain categories of personal and traffic data are not transferred outside India.

## Our Take

The lack of clarity on which Data Fiduciaries may qualify as SDFs introduces uncertainty in terms of compliance. Also, the potential for data localization may lead to conflicts with data privacy laws in foreign jurisdictions that require access to all processed data.

# DATA PRINCIPAL (DP)

According to the DPDP Act, a “Data Principal” is the person whose personal data is being collected. If the person is a child, it also includes their parents or legal guardian. If the person has a disability, it includes their legal guardian acting on their behalf.

**As a DP, you have several rights and protections:**

- Before a company processes your data, they must give you a detailed notice explaining what data they want to collect, why, and how it will be used (Rule 3).
- your data is breached, the company must inform you about the breach, its potential impact, and the steps they’re taking to mitigate it (Rule 7).
- Before your data is erased, the company must notify you, giving you the chance to act if you wish to keep it. You’ll receive a notification 48 hours before your data is set to be erased. This gives you a chance to log in or contact the fiduciary if you want to keep your data or take any necessary action before it’s deleted. (Rule 8).
- You have the right to access, correct, or delete your personal data. Companies must provide clear instructions on how to exercise these rights, including what identification details (like usernames or IDs) you need to verify your request (Rule 13).
- If you have concerns, companies must provide a clear process for filing complaints, including the time it will take to resolve them. You can also nominate someone you trust to manage these requests on your behalf (Rule 13).

## DP is a Parent or Child

Before a platform or service collects or uses the personal data of a child, the platform must get consent from the child's parent or lawful guardian. This process ensures that the parent is properly identified as an adult, and the platform follows due diligence in verifying the parent's identity before proceeding.

On January 7, Union Minister Ashwini Vaishnaw clarified that virtual tokens used for verifying children's data will be temporary and automatically deleted after a single use

**On January 7, Union Minister Ashwini Vaishnaw clarified that virtual tokens used for verifying children's data will be temporary and automatically deleted after a single use**

The platform can verify the parent's identity and age using two ways:

- Existing data (if the parent has already registered with the platform).
- New verification (if the parent is not registered, the platform will use government-issued details or a digital token provided by trusted authorities, such as Digital Locker, to verify the parent's identity and age).

| Case | Scenario | Parent's Registration Status | Verification Process | Verification Method |
|---|---|---|---|---|
| Case 1 | The child informs DF that she is a child | Parent is a registered user on DF's platform | Parent identifies herself and informs DF that her identity and age details were previously made available to DF | DF shall check to confirm that it holds reliable identity and age details of the parent |
| Case 2 | The child informs DF that she is a child | Parent is not a registered user on DF's platform | Parent identifies herself and informs DF that she is not a registered user on DF's platform | DF shall check that the parent is an identifiable adult using identity and age details issued by an entity entrusted by law or Government or a virtual token mapped to the same |
| Case 3 | The parent identifies herself as C's parent | Parent is a registered user on DF's platform | Parent identifies herself and informs DF that her identity and age details were previously made available to DF | DF shall check to confirm that it holds reliable identity and age details of the parent |
| Case 4 | The parent identifies herself as child's parent | Parent is not a registered user on DF's platform | Parent identifies herself and informs DF that she is not a registered user on DF's platform | DF shall check that the parent is an identifiable adult using identity and age details issued by an entity entrusted by law or Government or a virtual token mapped to the same |

**However, there are certain exceptions:**

- Certain entities, such as healthcare professionals, educational institutions, and daycare centres, can process children's data without parental consent if it is necessary for the child's well-being, safety, or learning. (Rule 11 Part A Schedule 4)

- The rules allow exceptions for processing children's data without parental consent in specific cases, such as for legal duties, public services, creating email accounts, blocking harmful content, or confirming if someone is a child. Data should only be used as necessary for these purposes. (Rule 11 Part B Schedule 4)

DP is Persons with Disabilities

If a person with a disability is unable to provide consent for their data processing, their legal guardian must give consent on their behalf. The platform must verify that the guardian is authorized by a court, a designated authority, or a local committee to make decisions for the person with a disability. (Rule 10)

## Our Take

The rules offer valuable protections for Data Principals, promoting transparency and empowering individuals with rights over their personal data. More clarity can be provided on how end users will be made aware of these rights to ensure effective implementation. The obligation for companies to notify individuals before erasing data is a positive step, but it would be beneficial to further specify the breach notification timeline for users. Currently, the rules mandate a 72-hour notification to the Data Protection Board, but the timeline for informing users remains unclear, which could create inconsistencies in the process.

Rules for protecting children's personal data also provide a positive framework by requiring verifiable parental consent before processing data, ensuring greater control for parents over their children's information. However, the rules could benefit from more clarity on acceptable verification methods beyond digital lockers and on how data should be managed once a child becomes an adult. Also, parents may find the frequent need to verify their identity using government-issued identification or digital tools like Digital Locker burdensome. This process could be challenging for some, especially if they are not comfortable with digital platforms or face difficulties in navigating these systems.

# CONSENT MANAGER

Under Section 2 of the DPDP Act, a Consent Manager (CM) is a person or entity registered with the Data Protection Board of India. Its primary role is to help individuals (Data Principals) give, manage, review, and withdraw their consent for the use of their personal data. The CM provides a clear, simple, and user-friendly platform to facilitate this process.

## Who Oversees the CM?

To become a registered CM, a person must apply to the Data Protection Board (DPB) and provide the required information. The Board will review the application and, if everything is in order, approve the registration and publish the details. If the conditions are not met, the application will be rejected with reasons given. Once registered, the CM must follow specific rules and obligations. If the Board finds that the CM is not following these rules, it can ask the manager to make corrections. In cases where it is needed to protect Data Principals, the Board can suspend or cancel the registration, after hearing from the CM. The Board can also ask the CM for additional information when necessary. (Rule 4)

## Obligations of CM

CM allows a user to give consent for their personal data to be processed. This can be done directly by the user to a company (Data Fiduciary) or through another company that holds the data with the user's permission.

- Direct Consent: X uses the Consent Manager's platform (P) to directly give consent to Bank B1 to access her bank statement.
- Routed Consent: X uses a P to give permission for her bank statement to be shared with

Bank B1. However, since X's account is with Bank B2, the consent is routed through B2. X instructs B2 to send her bank statement to B1, and B2 carries out the request by providing the statement to B1.

The CM ensures that personal data shared through its platform is not readable by it and maintains records of consent given, denied, or withdrawn, notices related to consent, and data shared with others. Individuals can access their consent records in machine-readable form, with records kept for at least seven years. The manager provides services through a website or app and cannot outsource its responsibilities. It must implement security measures to prevent data breaches and avoid any conflicts of interest with Data Fiduciaries. The manager is required to disclose information about its leaders, major shareholders, and any conflicts of interest while conducting regular audits and reporting results to the board. Ownership or control cannot be transferred without prior board approval. (Schedule 1 Part B)

**Qualification Criteria**

To become a registered Consent Manager, the applicant must meet the following key criteria:

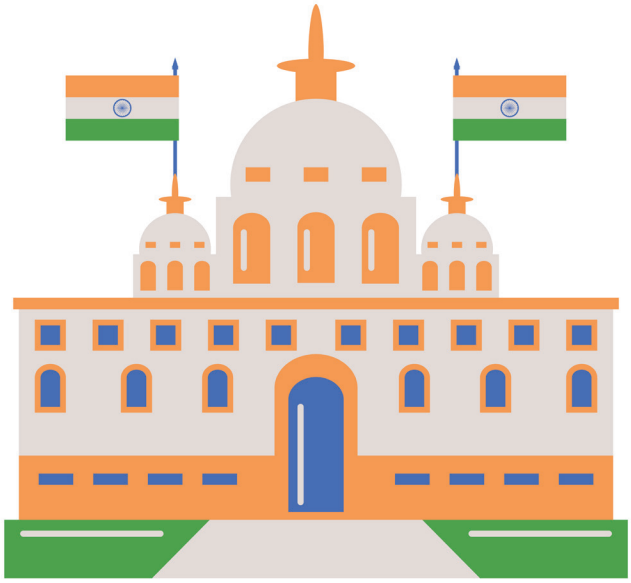
- The company must be incorporated in India.
- It should have the technical, operational, and financial capacity to meet its responsibilities.
- A minimum net worth of ₹2 crores is required.
- The management must have a reputation for fairness and integrity.
- Its business structure and earnings must be adequate.
- The operations must prioritize Data Principals' interests.
- The platform must comply with data protection standards.
- The platform must be independently certified for interoperability.
- Any policy changes require prior approval from the Board.
- (Schedule 1 Part A)

## Our Take

A CM under the Act is positioned as a central entity responsible for representing the Data Principal's interests and ensuring a standardized approach to consent management. However, the framework lacks clarity on whether data fiduciaries are required to mandatorily integrate with consent managers or if they may independently manage consents, creating ambiguity that could impact the framework's adoption and effectiveness. Furthermore, the operational model of consent managers is not fully articulated, leaving questions about how they will sustain their activities—whether through charges to DFs, DPs, or alternative mechanisms. Clarification on this would aid in effective implementation.

Given the technical and legal complexities involved, if businesses are required to onboard consent management platforms to meet compliance requirements under stringent data protection regulations, the demand for tools that support consent management and tracking is expected to grow. Larger organizations may find this transition more manageable due to their existing resources, while smaller entities may face challenges that could necessitate further investment in adopting these tools.

# GOVERNMENT AND ITS ENTITIES



- The government and its instrumentalities can process individuals' data (DPs) for issuing subsidies, benefits, services, certificates, licenses, or permits as outlined by law, government policies, or public funds. This processing must comply with the standards set in the Second Schedule, ensuring the data is processed lawfully, accurately, and only for specified purposes. (Rule 5)
- The government must inform DPs about the processing, provide clear contact information for inquiries, and offer mechanisms for DPs to exercise their rights under the Act. (Rule 5)
- The Central Government may issue orders to regulate data transfers to foreign countries or share with foreign-controlled entities. (Rule 14)
- The Central Government can request DFs or intermediaries to provide information for specific purposes, such as ensuring India's security or meeting legal requirements. If the information concerns national security, the DF or intermediary must obtain written consent from an authorised person before sharing it. (Rule 22)

## Our Take

The government or its instrumentalities can process personal data for other unrelated services if the data principal has already consented to one such service. While this provision could raise concerns about the broad and potentially overreaching scope of government power, there are safeguards in place, including requirements for lawful processing, purpose limitation, data minimization, ensuring data accuracy, implementing reasonable security measures, and ensuring accountability. Additionally, data fiduciaries must be informed about such processing, introducing an element of transparency and responsibility in the handling of personal data.

# DATA PROTECTION BOARD

Section 18 of the DPDP Act establishes the Data Protection Board. The rules 16-20 build on its specifics.

**Who decides who becomes the Chairperson and Members of the Board?**

A special, Search-cum-Selection Committee committee, led by the Cabinet Secretary, includes Secretaries of Legal Affairs and Electronics & IT, along with two experts. selects candidates for the Chairperson. For other Members: The committee is chaired by the Secretary of Electronics & IT, with similar composition.

**How is the salary and benefits for the Chairperson and Members decided?**

Their salary, allowances, and service conditions are mentioned in a specific schedule (Fifth Schedule).

**How do the Board meetings work?**

The Chairperson decides when and what will be discussed in the meetings. If the Chairperson is absent, a member chosen by others leads the meeting. Decisions are made when at least one-third of the Board is present, and a majority vote is required. In case of a tie, the Chairperson has the deciding vote. Members with conflicts of interest must not participate or vote on related issues. The Chairperson can also take emergency actions, but these need to be approved later.

**Can decisions be made without a meeting?**

Yes, if the Chairperson decides, decisions can also be made by sending the agenda to the Board members for their input.

**How quickly does the Board need to complete its work?**

The Board must finish its inquiries within six months, but it can ask for an additional three months if needed.

**How does the Board operate digitally?**

The Board mostly works online, using technology for meetings and proceedings, but it can still call people to give testimony under oath if necessary.

**How are officers and employees appointed to the Board?**

The Board can hire officers and employees, but they need approval from the Central Government first. The terms of their employment are listed in another schedule (Sixth Schedule).

## Our Take

The DPB holds significant promise as a central component of India's data governance framework, providing an independent body to address data-related issues and ensuring that all stakeholders, including the Government, are held accountable. However, concerns have been raised regarding its independence, as the central government is responsible for constituting the board. Since the Government may become a significant data fiduciary, questions have been raised about the DPB's ability to act as an impartial authority in cases involving the Government.

# APPELLATE TRIBUNAL

If someone is unhappy with a decision or direction made by the Board, they can appeal to the Appellate Tribunal established under Section 29(1) of the DPDP Act.

**How are appeals submitted to the Appellate Tribunal?**

Appeals must be submitted digitally, and there is a fee, similar to the fee under the Telecom Regulatory Authority of India Act, 1997. The fee can be waived by the Chairperson. Payments for the appeal must be made using UPI or other systems approved by the Reserve Bank of India (RBI). (Rule 21)

**How does the Appellate Tribunal work?**

The Appellate Tribunal operates independently from the Code of Civil Procedure, following its own rules and natural justice principles. It works digitally, reducing the need for physical presence, but can still call people to give testimony under oath.

# About **BharatGAIN**

BharatGAIN (Bharat Growth and Inclusion Network) is an independent think tank focused on overcoming barriers between policy creation and effective implementation across Indian industries. By connecting policymakers, industry leaders, and academia through rigorous research, evidence-based studies, and stakeholder engagements, we seek to combine best practices and behaviors to optimise the implementation of effective policies till the last mile.

With a commitment towards achieving inclusivity and digital equity, BharatGAIN offerings are a value addition for stakeholders working on creating robust regulatory frameworks, digital infrastructure, capacity building, and stakeholder alignment. By filling overlooked policy gaps and fostering collaborations, we aim to effect decisions that enable a technology-led growth, universalising access as a public good.

http://www.bharatgain.org | info@bharatgain.org