DPDP Rules

Reasonable security safeguards.—(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum,—

(a) appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data;

(b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor;

(c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;

(d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of databackups;

(e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;

(f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and

(g) appropriate technical and organisational measures to ensure effective observance of security safeguards.

The **Data Protection and Digital Privacy Rules, 2025 (DPDP Rules)** are expected to provide more detailed regulations in India regarding data privacy and protection, building upon the **Personal Data Protection Bill, 2019** (PDP Bill). While the exact specifics of the **DPDP Rules** are still pending, the expected framework would likely continue from the **PDP Bill**, and here are the primary **types of entities** that would be regulated under the DPDP rules:

**1. Data Fiduciaries**

* **Definition**: A **Data Fiduciary** is an entity (either a natural person or a legal body) that determines the purpose and means of processing personal data.
* **Responsibilities**: Data Fiduciaries have the primary responsibility for ensuring the lawful, transparent, and accountable processing of personal data. They must adhere to **data protection principles like consent, purpose limitation, data minimization, accuracy, and security.**
* **Examples**: Large corporations, online platforms (e.g., social media platforms, e-commerce platforms), banks, healthcare organizations, and government bodies that handle personal data.

**2. Data Processors**

* **Definition**: A **Data Processor** is an entity that processes personal data on behalf of a Data Fiduciary. The processor is bound by a contract that specifies the scope of data processing, security measures, and other obligations.
* **Responsibilities**: Data Processors are responsible for ensuring the security of the personal data they process and must comply with the instructions from the Data Fiduciary. They cannot use the data for any purposes other than what was agreed with the Data Fiduciary.
* **Examples**: Cloud service providers, data storage services, third-party analytics companies, and software-as-a-service (SaaS) providers that process personal data on behalf of organizations.

**3. Data Principals (Individuals)**

* **Definition**: A **Data Principal** is the individual whose personal data is being collected, processed, or stored. In the context of the DPDP Rules, the data principal has significant rights over their data, including consent management, data access, correction, and deletion.
* **Responsibilities**: While the Data Principal is not an entity regulated under the rules, they are the central figure whose privacy and rights are protected. Data Principals are empowered to:
  + Give or withdraw consent for the processing of their data.
  + Request access to or correction of their personal data.
  + Ask for the deletion of their data (under specific conditions, such as the "right to be forgotten").

**4. Data Protection Authority (DPA)**

* **Definition**: The **Data Protection Authority (DPA)** is an independent regulatory body set up to enforce the provisions of the DPDP Rules and ensure compliance with the data protection law.
* **Responsibilities**: The DPA is tasked with:
  + Monitoring and enforcing compliance with data protection regulations.
  + Handling complaints from Data Principals regarding data breaches or violations.
  + Imposing penalties and fines on entities that fail to comply with the data protection laws.
  + Providing guidance and issuing directives to Data Fiduciaries and Data Processors.
  + Raising awareness about data protection rights and obligations.
* **Examples**: This would be a new body specifically created under the DPDP framework and would work in coordination with other regulatory bodies.

**5. Service Providers**

* **Definition**: **Service Providers** are third parties that offer services to Data Fiduciaries or Data Processors, often related to processing, storage, or transmission of personal data.
* **Responsibilities**: These entities are generally required to follow data protection obligations similar to those of Data Processors. However, depending on the nature of their services, they may not always fall under the same direct legal responsibilities as Data Fiduciaries and Processors.
* **Examples**: Payment gateways, marketing agencies, customer support services, and third-party logistics providers.

**6. Critical Data Fiduciaries**

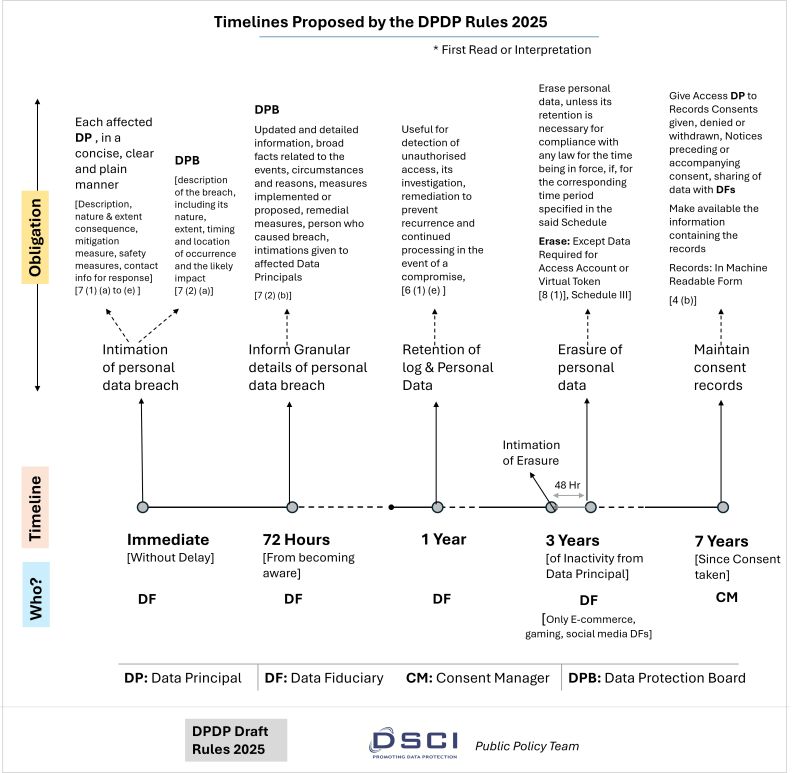
* **Definition**: A **Critical Data Fiduciary** is an entity that handles sensitive and large-scale personal data which could affect national security, public safety, or the economy.
* **Responsibilities**: Critical Data Fiduciaries would face stricter obligations under the DPDP Rules, including enhanced security measures and more stringent data localization and processing requirements.
* **Examples**: Telecom companies, major financial institutions, e-commerce platforms, and government services managing sensitive personal or health-related data.

**7. Third-Party Vendors**

* **Definition**: **Third-Party Vendors** are organizations or individuals that are subcontracted by a Data Fiduciary or Data Processor to handle some aspect of data processing or management.
* **Responsibilities**: Third-Party Vendors are subject to contractual obligations that bind them to comply with the data protection principles outlined in the DPDP Rules. They must ensure that the personal data is processed in accordance with the law and maintain appropriate security measures.
* **Examples**: Third-party marketing firms, analytics service providers, and other subcontractors who handle personal data.

**Conclusion**

The **DPDP Rules 2025** would likely regulate the various entities involved in the processing, storing, and handling of personal data within India. These rules aim to enforce the privacy rights of individuals (Data Principals) and impose responsibilities on entities like **Data Fiduciaries**, **Data Processors**, **Service Providers**, and **Critical Data Fiduciaries**. Additionally, the **Data Protection Authority** would act as a regulator to ensure compliance and safeguard individuals' data rights.



**Risk-Based Approach**: The bill adopts a risk-based approach, where the regulatory framework is more proportionate to the type and amount of data being processed.

## **Consent-Based Data Processing**

The default rule under the DPDP Act is that **data processing must be based on valid consent from the individual (Data Principal)**.

### ****Key Features of Consent****

* **Free, Specific, Informed, and Unambiguous**: Consent must be clear, with individuals knowing what data is collected and how it is used.
* **Explicit & Affirmative Action**: No pre-checked boxes or implied consent—users must actively agree.
* **Limited Scope**: Data can only be used for the purpose for which consent was given.
* **Easily Withdrawable**: Users can withdraw consent at any time, and the company must stop processing their data.

### ****Consent Manager****

* The act introduces **Consent Managers**, independent entities that help individuals manage and withdraw consent efficiently.
* These managers must be **registered with the Data Protection Board** and act as intermediaries between users and companies.

## **2. Processing Without Consent (Legitimate Uses)**

In certain cases, organizations **can process personal data without explicit consent**, including:

### ****Government Functions****

* National security, law enforcement, and disaster response.
* Subsidy or benefit schemes approved by the government.

### ****Employment-Related Data****

* Processing necessary for recruitment, payroll, or employee benefits.

### ****Compliance with Laws & Court Orders****

* If required by legal obligations, court orders, or regulatory compliance.

### ****Public Interest & Research****

* Processing for statistical, research, or archival purposes, provided privacy safeguards are in place.

## **3. Special Cases: Children's Data & Sensitive Data**

* **Parental Consent**: Data Fiduciaries must get **verifiable parental consent** before collecting data from children (under 18 years).
* **High-Risk Data Processing**: If a company is classified as a **Significant Data Fiduciary**, it may have additional obligations, such as appointing a **Data Protection Officer** and conducting impact assessments.

## **4. Accountability & Compliance**

* Companies must **store proof of consent** and be able to demonstrate compliance.
* If they process data without consent when it's required, they face **heavy penalties**.

### ****Rights of Data Principals (Individuals) Under the DPDP Act****

The **Digital Personal Data Protection (DPDP) Act** grants individuals (called **Data Principals**) several rights over their personal data. These rights ensure transparency, control, and accountability in how personal data is processed.

## **1. Right to Access Information**

* Individuals can request details about:
  + What personal data is being collected.
  + How their data is being processed and for what purpose.
  + Any third parties with whom their data has been shared.

📌 **Example:** If a user signs up for an online service, they can ask the company what data they have stored about them.

## **2. Right to Correction & Erasure**

* Individuals can:
  + Request correction of inaccurate or outdated data.
  + Update their personal data if it is incomplete.
  + Ask for **erasure (deletion)** of their personal data when it's no longer needed.

📌 **Example:** A user can request a bank to update their address or remove old contact details.

## **3. Right to Grievance Redressal**

* If a user’s data is misused or their rights are violated, they can file a **grievance (complaint)** with the Data Fiduciary (company handling the data).
* If the company does not respond satisfactorily, users can escalate the issue to the **Data Protection Board of India**.

📌 **Example:** If an online shopping website continues sending promotional emails despite unsubscribing, the user can file a complaint.

## **4. Right to Nominate**

* Individuals can **nominate someone** (such as a family member) to exercise their data rights **in case of death or incapacity**.
* This ensures that personal data is managed properly even if the individual is unable to take action.

📌 **Example:** A person can appoint their spouse to manage their data rights in case they are unable to do so.

### ****Limitations on Rights****

* Rights may be restricted in cases involving:
  + National security and law enforcement.
  + Prevention of fraud and cybercrimes.
  + Compliance with legal obligations.

### ****How These Rights Benefit Users****

✅ **More control over personal data**  
✅ **Transparency from companies**  
✅ **Stronger privacy protection**

Would you like details on how to **enforce these rights** or the **penalties for violations**? 🚀

### ****Obligations of Data Fiduciaries (Organizations Handling Personal Data) Under the DPDP Act****

The **Digital Personal Data Protection (DPDP) Act** defines strict responsibilities for **Data Fiduciaries**—companies, organizations, or individuals that collect, store, and process personal data. These obligations ensure that personal data is handled securely, lawfully, and transparently.

## **1. Obtaining Valid Consent**

* **Must obtain clear, informed, and specific consent** from users before collecting personal data.
* Users must be told:
  + What data is being collected.
  + How it will be used.
  + Their rights to withdraw consent.
* Data Fiduciaries must **maintain proof of consent**.

📌 **Example:** A social media app must explicitly ask for permission before collecting location data.

## **2. Purpose Limitation & Data Minimization**

* Data can **only be used for the specific purpose** for which it was collected.
* Organizations must **not collect excessive or unnecessary personal data**.

📌 **Example:** An e-commerce site should not collect medical history if it only needs a shipping address.

## **3. Storage Limitation & Data Deletion**

* Personal data **must not be stored indefinitely**—it should be deleted when no longer needed.
* Users can request deletion of their data under the **Right to Erasure**.

📌 **Example:** A financial service must delete KYC (Know Your Customer) documents once the legal retention period expires.

## **4. Data Security Measures**

* Must implement **reasonable security safeguards** to prevent:
  + Data breaches.
  + Unauthorized access or misuse of data.
* If a **data breach occurs**, the organization must **notify the Data Protection Board of India** and affected users.

📌 **Example:** A cloud storage provider must encrypt user data and ensure secure authentication.

## **5. Grievance Redressal Mechanism**

* Must provide an easy way for users to:
  + File complaints about misuse or unauthorized processing.
  + Get their issues resolved within a **reasonable time frame**.

📌 **Example:** A fintech company must offer a helpdesk for users to raise concerns about unauthorized transactions.

## **6. Additional Obligations for Significant Data Fiduciaries**

Some organizations handling **large volumes of sensitive personal data** are classified as **Significant Data Fiduciaries** (SDFs). They have extra obligations, such as:

* **Appointing a Data Protection Officer (DPO)** to oversee compliance.
* **Conducting regular Data Protection Impact Assessments (DPIA)**.
* **Carrying out periodic security audits**.

📌 **Example:** A major bank processing financial data of millions of users must have a dedicated Data Protection Officer.

## **7. Cross-Border Data Transfers**

* Data Fiduciaries can transfer personal data outside India **unless restricted by the government**.
* They must ensure that foreign entities follow **similar levels of data protection**.

📌 **Example:** A global IT company must comply with Indian data laws when storing Indian user data on foreign servers.

### ****Non-Compliance & Penalties****

❌ Failure to comply with these obligations can result in **hefty penalties**—up to **₹250 crore** for serious violations.

Would you like details on **penalties and enforcement** next? 🚀

### ****Penalties & Enforcement Under the DPDP Act****

The **Digital Personal Data Protection (DPDP) Act** imposes **strict penalties** on organizations that violate data protection rules. The penalties vary based on the type and severity of the violation.

## **1. Penalties for Non-Compliance**

| **Offense** | **Maximum Penalty** |
| --- | --- |
| **Failure to implement security safeguards, leading to a data breach** | ₹250 crore |
| **Failure to notify users & authorities of a data breach** | ₹200 crore |
| **Non-compliance with obligations related to children's data** | ₹200 crore |
| **Failure to fulfill individual rights (like access, correction, or erasure requests)** | ₹150 crore |
| **Non-compliance with obligations of Significant Data Fiduciaries (SDFs)** | ₹50 crore |
| **Failure to prevent unauthorized data processing** | ₹10 crore |
| **Breach of other DPDP rules and regulations** | As prescribed by the Data Protection Board |

📌 **Example:** If a social media company suffers a data breach but does not inform users, it could face a ₹200 crore fine.

## **2. Enforcement Mechanism**

### ****Data Protection Board of India (DPBI)****

* The **Data Protection Board** is the primary enforcement authority under the DPDP Act.
* It has the power to:
  + **Investigate complaints** and order penalties.
  + **Direct companies to take corrective actions**.
  + **Suspend or restrict data processing** if necessary.

### ****Complaint Process****

1. A **Data Principal (user)** files a complaint with the **Data Fiduciary (company)**.
2. If not resolved, the user can escalate the complaint to the **Data Protection Board of India (DPBI)**.
3. The DPBI investigates and imposes penalties if violations are found.

📌 **Example:** If a bank refuses to delete a user’s personal data upon request, the user can escalate the issue to the DPBI.

## **3. Criminal & Legal Consequences**

* In addition to fines, companies may face **operational restrictions**, such as suspension of data processing.
* Government authorities may impose **additional penalties for national security or fraud-related violations**.

### ****How Organizations Can Avoid Penalties****

✅ **Implement strong data security measures**  
✅ **Ensure clear and valid consent**  
✅ **Respond to user requests on time**  
✅ **Comply with cross-border data transfer rules**

Would you like guidance on **how businesses can ensure compliance** with DPDP rules? 🚀