Sarvaank

Law Decoded for *Entrepreneurs*

ANALYSIS ON DIGITAL PERSONAL DATA PROTECTION RULES 2025

PART-1

In the contemporary digital landscape, data has emerged as a powerful resource, often referred to as being "the new oil". The growing volume of personal data calls for a robust and comprehensive legal framework to address concerns surrounding privacy, security, and ethical data usage.

India's first significant step towards data protection came with the introduction of the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, formulated under Section 43A of the Information Technology Act, 2000*. These rules were aimed at protecting personal data by setting guidelines for the collection, storage, and processing of sensitive personal data. They defined Personally Identifiable Information ("**PII**") and outlined the responsibilities of entities handling such data, ensuring that reasonable security measures were implemented to prevent data breaches.

Further, a major milestone in India's data privacy journey occurred in 2017 when the Supreme Court delivered a landmark verdict in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[1]. In this case, the Court ruled that the right to privacy is a fundamental right under **Article 21** of the Indian Constitution. This ruling affirmed the constitutional protection of personal privacy, including the protection of data, in the digital context. It was a significant step towards recognizing the importance of individual privacy in an increasingly interconnected world.

Following the Puttaswamy judgment, other key rulings, including the Swaminathan judgment, stated the necessity of maintaining individual privacy in the context of various government programs, such as Aadhaar. These cases emphasized the need for strict safeguards, transparency, and accountability in the processing of personal data, particularly in government-led initiatives.

The global regulatory landscape also played an influential role in shaping India's approach to data privacy. The introduction of the *European Union's General Data Protection Regulation (GDPR)* in 2018 set new standards for data protection. GDPR's framework, which emphasizes transparency, user consent, accountability, and data portability, provided a model for countries worldwide, including India, to consider when drafting their own privacy laws. The GDPR's strict requirements for data processing and its emphasis on user rights directly influenced India's legal discourse on data privacy.

In response to the increasing awareness and global movement towards data security, the Standing Committee on Communications and Information Technology, chaired by Mr. Prataprao Jadhav, submitted a report titled *Citizens' Data Security and Privacy* on August 1, 2023. The report outlined critical issues related to data privacy and security, urging the government to adopt a comprehensive legal framework for the protection of citizens' personal data. The Committee highlighted the necessity of aligning India's data protection policies with global standards, particularly those set by GDPR, while considering the country's specific challenges in the digital ecosystem.

Another important contribution to the evolution of data privacy in India came from the **Swaminathan Commission**, which made several key recommendations on balancing technological advancements with individual rights. The Commission emphasized the importance of enacting laws that would

[1] Supreme Court, Writ Petition (Civil) No 494 Of 2012

safeguard personal data while facilitating innovation. Its suggestions helped steer the policy-making process, laying the groundwork for future legal developments.

The culmination of India's efforts to create a legal framework for data protection came with the enactment of **the Digital Personal Data Protection Act, 2023, (the DPDP Act or the Act**) which received presidential assent on August 11, 2023. This Act establishes a comprehensive framework for the collection, processing, and storage of personal data, prioritizing individual rights, data security, and transparency. It outlines the roles and responsibilities of data fiduciaries, and sets strict guidelines on user consent, data processing, and breach notification.

On January 3, 2025, the Draft Digital Personal Data Protection Rules, 2023 (the Rules or Draft Rules) were released for public consultation. These Rules aim to complement the Act by providing detailed provisions regarding the implementation of the Act. Key highlights of the Draft Rules include specific guidelines on the right to access, correction, and erasure of personal data, including the personal data of children and the processes for data fiduciaries to ensure compliance with the law. The rules also provide clarity on cross-border data flows, data breach notifications, and the establishment of data protection officers. Together, these developments reflect India's evolving approach to data privacy, balancing the need for protecting citizens' rights with the demands of an increasingly digital economy.

One of the key elements in the DPDP Act are the terms Data Principals and Data Fiduciary, who govern the entire DPDP Act.

Data Fiduciary and Data Principal

At the core of the DPDP Act, it recognized two pivotal entities: the Data Principal and the Data Fiduciary. The **Data Principal**, as defined under the act, referred to the individual to whom personal data related, encompassing children through their parents or lawful guardians and individuals with disabilities through lawful guardians, acting on their behalf[2]. Meanwhile, the **Data Fiduciary** was identified as any entity determining the purpose and means of data processing, carrying an obligation to handle personal data responsibly[3].

Under this Act, the dynamic between the Data Principal and the Data Fiduciary aimed to create a transparent and accountable ecosystem for data management. The provisions ensured that the Data Principal retained significant control over their data through rights like consent, correction, and grievance redressal, while Data Fiduciaries were tasked with safeguarding data through compliance, security measures, and responsible usage protocols.

Provisions for Data Fiduciary Under DPDP Act:

As stated above, the Act introduced the concept of Data Fiduciary as a fundamental entity in its regulatory framework. Defining the Data Fiduciary as any person or organization that determines the

[2] Section 2(j), Digital Personal Data Protection Act, 2023
[3] Section 2(i), Digital Personal Data Protection Act, 2023

purpose and means of processing personal data, either independently or in collaboration with others. The Act imposed a series of comprehensive obligations on Data Fiduciaries, these obligations include:

Lawful Processing of Personal Data:

Data Fiduciaries are required to process personal data only under specific lawful grounds[4]:

- Consent-based Processing: Data must be processed with the explicit, informed consent of the Data Principal.

- Legitimate Uses: Certain non-consensual processing is permitted for purposes such as compliance with legal obligations, responding to emergencies, or public welfare (Section 7).

Provision of Notice

Before collecting personal data, a Data Fiduciary must provide the Data Principal with a notice detailing, the types of personal data being collected, the purpose for which it is being processed, the methods available for the Data Principal to exercise their rights, such as access, correction, or grievance redressal, and the process for filing complaints with the Data Protection Board of India. The **notice must be presented in clear, plain language, accessible in English and other languages specified in the Eighth Schedule of the Constitution of India**.[5]

Consent Management

Consent must be obtained from the Data Principal, and such consent must be free, specific, informed, and unambiguous. The Act allows the **withdrawal of consent at any time, and the process for withdrawal must be as simple as providing consent was.** Upon withdrawal, Data Fiduciaries must cease processing the personal data of the Data Principal, unless required otherwise by law[6]

Legitimate Use

The Act permits **Data Fiduciaries to process personal data without explicit consent under specific legitimate purposes, balancing individual rights with societal and administrative needs**. These include processing of data when data is voluntarily provided by the Data Principal for a specific purpose and no objection is raised, or processing for issuing subsidies, benefits, or certificates, provided the data is already available in notified government databases or consent was previously given. Data can be processed for statutory functions or activities safeguarding sovereignty, public order, or security or to fulfill obligations under laws or court orders. Further, the data can be processed for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual and lastly for ensuring workplace safety, preventing corporate espionage, or delivering employment-related benefits.[7]

General Obligations of Data Fiduciaries[8]

[4] Section 4, Digital Personal Data Protection Act, 2023
[5] Section 5, Digital Personal Data Protection Act, 2023
[6] Section 6, Digital Personal Data Protection Act, 2023
[7] Section 7, Digital Personal Data Protection Act, 2023
[8] Section 8, Digital Personal Data Protection Act, 2023

Provisions	Description
Responsibility for Compliance	Data Fiduciaries are solely responsible for ensuring compliance with the provisions of the Act, regardless of any agreements with Data Processors or the actions of Data Principals.
Engagement of Data Processors	Data Fiduciaries may engage Data Processors to carry out specific data processing activities on their behalf. Such engagements must be governed by valid contracts, ensuring that the Data Processor adheres to the obligations set by the Act.
Accuracy and Completeness	Data Fiduciaries are required to ensure the accuracy, completeness, and consistency of personal data when it influences decisions affecting the Data Principal, or when such data is disclosed to another Data Fiduciary.
Organizational Measures	Data Fiduciaries must implement appropriate technical and organizational measures to effectively comply with the Act.
Security Safeguards	Data Fiduciaries must take reasonable security measures to protect personal data in their possession or under their control, including data handled by their Data Processors.
Data Breach	In the event of a personal data breach, Data Fiduciaries must notify the Data Protection Board of India and inform the affected Data Principals. The notification must follow the prescribed form and manner, ensuring that Data Principals can take necessary precautions.
Data Retention and Erasure and Data Retention Period	Data Fiduciaries are prohibited from retaining personal data beyond the period required to fulfill the specified purpose, except where retention is necessary for compliance with laws. Data Fiduciary must: 1. Erase personal data upon the withdrawal of consent by the Data Principal or when the specified purpose is no longer served. 2. Ensure that their Data Processors also erase the data. Exceptions: Laws requiring specific retention periods, such as tax or audit regulations, take precedence. A purpose is deemed no longer served if: 1. The Data Principal does not approach the Data Fiduciary for performance of the specified purpose within a prescribed time. 2. The Data Principal does not exercise their rights concerning the data within that time frame. Different retention periods may apply based on classes of Data Fiduciaries and the nature of the purpose for processing.

Contact Information for queries	Data Fiduciaries must publish business contact details of a Data Protection Officer (for Significant Data Fiduciaries), an authorized representative who can respond to queries regarding the processing of personal data.
Grievance Redressal mechanism	Data Fiduciaries must establish a mechanism to address grievances from Data Principals, ensuring prompt and effective redressal within a prescribed timeline, accessibility and transparency in the grievance resolution process.

Processing of Personal Data of Children

Data Fiduciaries are subject to heightened obligations when processing personal data belonging to children (individuals below 18 years of age) or persons with disabilities who have lawful guardians. **Before processing a child's data, verifiable consent must be obtained from a parent or lawful guardian**. Data Fiduciaries are barred from engaging in behavioural tracking of children, targeted advertising directed at children and any processing that is likely to cause detrimental effects to a child's well-being.[9]

Obligations of Significant Data Fiduciaries

Significant Data Fiduciary is a Data Fiduciary designated by the Central Government based on several criteria, including the volume and sensitivity of personal data processed, the potential risk to Data Principals, and the impact on public order, sovereignty, and security. Significant Data Fiduciaries are subject to additional compliance measures, including the appointment of a **Data Protection Officer** who must be based in India, and shall report directly to the Board of Directors or equivalent authority and shall serve as a point of contact for grievance redressal under the Act.

Significant Data Fiduciaries must appoint an **independent data auditor** to evaluate compliance with the Act and identify risks in their data processing activities. Periodic Data Protection Impact Assessments (DPIAs) involve assessing risks associated with data processing activities and implementing measures to mitigate these risks.

Additionally, Significant Data Fiduciaries must adhere to additional reporting and compliance protocols, as prescribed by the Central Government. They are also required to periodically report their compliance status to regulatory authorities.[10]

Data Fiduciaries' Enhanced Obligations Draft Digital Personal Data Protection Rules, 2025:

The Draft Digital Personal Data Protection Rules, 2025, (Draft Rules) complement the Digital Personal Data Protection Act, 2023, by elaborating on the obligations of Data Fiduciaries to ensure a robust data protection framework.

[9] Section 9, Digital Personal Data Protection Act, 2023

[10] Section 10, Digital Personal Data Protection Act, 2023

Provision	Description
Notice to Data Principal	Data Fiduciaries must provide clear and plain notices to Data Principals before collecting personal data. The notice should include an itemized description of personal data being collected and the specified purpose and description of goods or services enabled by such processing.[11]
Processing Personal Data for Subsidies and Benefits	State entities may process personal data to provide subsidies, benefits, or services under legal or policy frameworks. Such data processing must comply with the standards in the Second Schedule, ensuring lawful and necessary use.[12]
Security Safeguards	Data Fiduciaries must implement robust security safeguards to protect personal data, including encryption, obfuscation, or masking, and control access to computer resources. They must maintain logs for one year to monitor and detect unauthorized access, investigate breaches, and prevent recurrence, while ensuring data continuity through backups. Contracts with Data Processors must mandate adherence to these safeguards, supported by appropriate technical and organizational measures.[13]
Data Breach Notification	When a Data Fiduciary becomes aware of a personal data breach, they must promptly inform affected Data Principals and the Data Protection Board. Notifications to Data Principals must be concise and clear, detailing the breach's nature, extent, timing, and location, its potential consequences, mitigation measures taken, recommended safety steps, and a contact for further queries. The Board must be notified immediately with a breach description and updated details within 72 hours, including its cause, mitigating measures, and remedial actions. A report on notifications sent to Data Principals must also be submitted. The term "user account" encompasses all registered profiles or contact methods used by Data Principals to access the Data Fiduciary's services.[14]
Retention and Erasure of Data	A Data Fiduciary must erase personal data when the specified purpose for processing is no longer served, as outlined in the Third Schedule, unless retention is required by law. If a Data Principal does not interact with the Data Fiduciary or exercise their rights within the specified time, the data must be deleted. The Data Fiduciary must notify the Data Principal at least 48 hours before erasure, unless the Data Principal logs into their account or contacts the Fiduciary to continue the purpose. A "user account" includes

[11] Rule 3, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[12] Rule 5, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[13] Rule 6, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[14] Rule 7, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*

	any registered profiles or communication methods used to access the Fiduciary's services.[15]
Contact Information for Queries	Data Fiduciaries must publicly display contact information on their website or app for the Data Protection Officer or a designated person responsible for addressing queries related to personal data processing. This contact information should also be included in every response to communications from a Data Principal exercising their rights under the relevant Act.[16]
Processing Children's Information	A Data Fiduciary must implement appropriate technical and organizational measures to obtain verifiable consent from a child's parent before processing their personal data. The Data Fiduciary must ensure due diligence to verify that the individual claiming to be the parent is an adult and identifiable, if necessary, for legal compliance. Verification can be done through: 1. Reliable identity and age details already available with the Data Fiduciary, or 2. Voluntarily provided identity and age details, or a virtual token, issued by a legally authorized entity (such as the Central or State Government) or a person appointed for such purposes, and verified through services like Digital Locker.[17]
Additional Obligations for Significant Data Fiduciaries	A Significant Data Fiduciary has the following additional obligations: 1. Every 12 months, a Significant Data Fiduciary must conduct a Data Protection Impact Assessment (DPIA) and an audit to ensure compliance with the relevant laws and rules, and must provide a report to the Board, highlighting significant findings from the assessment and audit. 2. The Data Fiduciary must ensure that any algorithmic software it uses for processing personal data does not pose a risk to the rights of Data Principals. 3. The Data Fiduciary must take measures to ensure that personal data, as specified by the Central Government (based on committee recommendations), is processed under specified restrictions.[18]

[15] Rule 8, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[16] Rule 9, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[17] Rule 10, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[18] Rule 12, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*

Cross-Border Data Transfers	The transfer of personal data outside India, whether processed by a Data Fiduciary within India or outside India in relation to activities offering goods or services to Data Principals in India, is subject to restrictions. The Data Fiduciary must comply with specific requirements set by the Central Government, through general or special orders, when making such personal data available to any foreign state, its agencies, or any entities under the control of that state.[19]
Exemptions for research and Statistical Purposes	The provisions of the Act do not apply to the processing of personal data if it is necessary for research, archiving, or statistical purposes, as long as the processing is carried out in accordance with the standards specified in the Second Schedule of the Act.[20]

Rights and Duties of the Data Principal under the Act and the Rules

The idea of the Data Principal establishes the individual as the rightful owner of their personal data, ensuring data privacy and user empowerment in the digital age. This framework underlines the principle that individuals possess inherent authority over their data, thereby challenging previously unchecked control. Through rights such as access, correction, portability, and erasure, Data Principals can actively manage and safeguard their personal data. Consent forms the cornerstone of data processing, empowering individuals to grant, withdraw, or modify consent seamlessly, thus retaining control throughout the data lifecycle.

Right to Obtain information

Data Principals have the right to request and obtain specific information from Data Fiduciaries regarding the processing of their personal data. **To facilitate the exercise of rights under the Act, Data Fiduciaries, and where applicable, Consent Managers, are required to publish clear guidelines on their website or app**. **These guidelines must specify the process for submitting requests and outline any necessary details, such as usernames or other identifiers, required to verify the identity of Data Principals in accordance with the terms of service[21]**. A summary of the personal data being processed and the associated processing activities, as well as the identities of all Data Fiduciaries and Data Processors with whom the data has been shared, accompanied by a description of the shared data. Additionally, data fiduciaries must provide any other prescribed information related to the personal data and its processing. However, disclosures regarding shared data are exempted when such sharing is authorized by law for purposes such as preventing, detecting, investigating, prosecuting offenses, handling cyber incidents, or punishing offenses[22].

The term "**identifier**" refers to any sequence of characters assigned by the data fiduciary to recognize a data principal. This may include identifiers such as a customer identification file number, customer acquisition form number, application reference number, enrolment ID, or license number, which facilitate the identification process[23].

[19] Rule 14, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[20] Rule 15, Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[21] Rule 13(1), Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[22] Section 11, Digital Personal Data Protection Act, 2023 (No. 22 of 2023)
[23] Rule 13(5), Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*

Right to Correction and Erasure

Data Principals have the right to request the access, correction, completion, updating, or erasure of their personal data **by directly contacting** the data fiduciary[24]. Upon receiving such a request, data fiduciaries are obligated to correct any inaccurate or misleading data, complete incomplete data, update data as necessary, and erase data unless its retention is required for specific purposes or to comply with prevailing legal obligations[25].

Right to Grievance Redressal

Data Principals are entitled to accessible grievance redressal mechanisms provided by a Data Fiduciary or Consent Manager. To ensure effective grievance resolution, Data Fiduciaries must establish transparent timelines and implement robust technical and organizational safeguards, grievances must be **addressed within a prescribed timeframe**[26]. Data principals are required to exhaust these mechanisms before approaching the Data Protection Board ("**Board**")[27].

Right to Nomination

Data Principals reserve the right to **nominate any other individual to exercise their rights in the event of their death or incapacity[28].** This nomination must be carried out in a prescribed manner, adhering to the terms of service of the relevant Data Fiduciary and applicable legal provisions. Data Fiduciaries are required to provide clear means and specify the necessary particulars to facilitate the nomination process, ensuring compliance with the Act and its associated Rules[29].

Obligations of the Data Principal

Data Principals are required to adhere to certain responsibilities while exercising their rights under the Act. They must comply with all applicable laws and avoid impersonating others when providing personal data for specified purposes. Additionally, they are prohibited from suppressing material information when submitting personal data for documents, unique identifiers, or proofs issued by the State or its agencies. **Data Principals must refrain from filing false or frivolous grievances with a Data Fiduciary or the Board and are obligated to provide only verifiably authentic information when exercising rights such as correction or erasure of personal data**[30].

India's Digital Personal Data Protection Act, 2023, marks a critical step toward establishing a secure and accountable digital ecosystem. By emphasizing individual rights, organizational accountability, and stringent data protection measures, the Act aligns with global best practices while addressing India's unique needs. Its implementation is set to enhance trust in data-driven technologies, promote responsible innovation, and strengthen the digital economy, paving the way for a more secure and equitable digital future.

****

For more information visit www.sarvaankassociates.com

[24] Rule 13(2), Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[25] Section 12, Digital Personal Data Protection Act, 2023 (No. 22 of 2023)
[26] Rule 13(3), Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[27] Section 13, Digital Personal Data Protection Act, 2023 (No. 22 of 2023)
[28] Section 14, Digital Personal Data Protection Act, 2023 (No. 22 of 2023)
[29] Rule 13(4), Digital Personal Data Protection Rules, 2025 (Draft), *3rd January, 2025*
[30] Section 15, Digital Personal Data Protection Act, 2023 (No. 22 of 2023)