



SARAF AND
PARTNERS
LAW OFFICES

REDESIGNING PRIVACY

**The Digital
Personal Data
Protection Rules,
2025 (Draft): A
Deep Dive**



REDESIGNING PRIVACY



The Digital Personal Data Protection Act, 2023 (**DPDPA**) was enacted by the legislature on 11th August 2023 to regulate the processing of digital personal data in the country. The objective of the legislation is that digital personal data is processed in a manner that recognizes both the right of the individuals to protect their personal data and the need to process such personal data for lawful purposes. On 3rd January 2025, after a period of almost 16 months, the Ministry of Electronics and Information Technology (**MeitY**) has published the much awaited draft of 'The Digital Personal Data Protection Rules, 2025' (**DPDP Rules**) for public consultation. The deadline for submitting comments on the DPDP Rules is 18th February 2025. A brief overview of the DPDP Rules is provided below:

1. Staggered Implementation

The DPDP Rules provide for a staggered implementation plan. Some of these rules will become effective upon publication of the DPDP Rules in the official gazette (Rules 1 to 2, and 16 to 20 deal with the establishment of the Data Protection Board), while the remaining rules (Rules 3 to 15, 21, and 22 dealing with key compliance requirements and mechanisms for enforcement of rights) are set to take effect at a later date to be decided by the Central Government.

2. Notice Requirements for Data Fiduciaries

Data Privacy Notices issued to Data Principals must be clear, concise, and standalone. The requirements include:

- **Independent Presentation:** The notice must be presented and understandable independently of other information provided by the Data Fiduciary and must not rely on other documents for its meaning and must include all necessary information upfront.
- **Itemized Details:** Data fiduciaries must list the types of personal data being processed and its specific purposes as well as an itemized description of the goods or services facilitated by the processing of the specified personal data.
- **Communication link:** Notice must include direct links to platforms where the Data Principals can withdraw consent with ease, exercise their rights, or raise complaints to the Data Protection Board.

These notice requirements ensure transparency and empowers individuals to make informed decisions about the processing of their personal data.

REDESIGNING PRIVACY



3. Registration and Role of Consent Managers

Consent managers are platforms which shall enable the Data Principals to give consent to the processing of their personal data by a Data Fiduciary onboarded onto the platform of the consent manager.

- **Registration Requirements:** Consent managers must meet the specified conditions including having a net worth of at least ₹2 Crores and have sufficient technical, operational and financial capacity to fulfil their obligations as a consent manager.
- **Core Obligations:** Consent managers must maintain records of consents including privacy notice; ensure personal data being shared is not readable by it; develop a website or app for providing services to Data Principals; and adopt measures to avoid conflicts of interest.
- **Data Handling Security:** The DPDP Rules prescribe that consent managers implement reasonable security safeguards to prevent personal data breaches.
- **Fiduciary Capacity:** Consent Managers must act in a fiduciary capacity and in the interests of the Data Principal.
- **Accountability Measures:** The Data Protection Board can instruct the consent managers to ensure compliance, request information, and suspend registration for non-compliance.

4. Processing by the State and Its Instrumentalities

The DPDP provides that the State and its instrumentalities can process personal data for the purpose of issuing subsidies, benefits, services, certificates, licenses, or permits without the explicit consent of the data principals. The DPDP Rules provide the standards to be followed by the State and its instrumentalities for such processing of personal data.

- **Restricted Processing:** The processing must be limited to the intended purpose, such as issuing a certificate or providing a subsidy under a law or policy.
- **Data Minimization:** Processing is limited to such personal data as necessary for achieving the purposes set out.
- **Accuracy:** Data fiduciary to make reasonable efforts to ensure accuracy of personal data.
- **Storage Limitation:** Personal data is retained till required for such uses or achieving such purposes.

REDESIGNING PRIVACY



- **Security:** Data fiduciaries to implement reasonable security safeguards to prevent personal data breaches including in respect of processing undertaken by a third-party data processor.

5. Security Safeguards for Personal Data

Data Fiduciaries are required to implement reasonable security measures to protect personal data from personal data breaches. These measures include at minimum:

- **Technical Safeguards:** Data Fiduciaries must implement appropriate security measures for securing personal data through measures such as encrypting, masking, obfuscation or using virtual tokens to secure personal data.
- **Access Controls:** Systems must allow only authorized personnel to access personal data, with continuous monitoring through detailed logs.
- **Continuity of operations:** Data Fiduciaries must ensure continued processing in the event of a personal data breach, through backups.
- **Incident Management:** Breach logs must be retained for at least one year to ensure effective investigation and remediation.
- **Organizational measures:** Implement appropriate technical and organizational measures to ensure effective observance of security standards.
- **Data Processing Agreements:** Data Fiduciaries are required to include provisions for taking reasonable security safeguards in their contracts with data processors, to foster accountability across the ecosystem.

6. Data Breach Notification

The DPDP Rules provide that any personal data breach must be promptly reported to:

- **Affected Data Principals:** Data Principals must be notified in a concise, clear and plain manner and without delay, with details about the nature of the and extent of breach, its potential impact, steps taken to mitigate risks and business contact information of a person who will respond to the queries of the data principals.

REDESIGNING PRIVACY



- **The Data Protection Board:** Data fiduciaries must promptly submit a preliminary notification followed by a detailed report within 72 hours to the Data Protection Board in respect of the breach. The initial notification must contain information about the nature, extent, timing and location of occurrence and the likely impact of the breach. The detailed report must contain broad facts relating to the events, circumstances and reasons for the breach, measures implemented to mitigate risk, any findings regarding who caused the breach, remedial measures to prevent recurrence and a report regarding intimation to the affected data principles.

This ensures a high degree of transparency, accountability and the importance of timely communication in mitigating risks associated with personal data breaches.

7. Rights of Data Principals

- The DPDP Rules details the procedure for exercising rights by data principals, reinforcing their control over personal data. Data fiduciaries must prominently display the following on their website or app:
- The procedure through which a data principal can make a request for exercising her rights.
- The method of identifying the data principal making the request using username or any other identifier.
- Method to nominate another individual to exercise rights of the data principal

The DPDP Rules do not provide a timeline for the Data Fiduciaries to respond to the requests. However, Data Fiduciaries and Consent Managers are required to specify timelines for responding and taking action under their grievance redressal system, which shall be published on their website and/or app. Similarly, the process for nomination may be specified in the terms of service, or as per any other applicable law. Every Data fiduciary must publish the business contact information of a person (or Data Protection Officer) in response to every request for exercise of rights by the Data Principal to respond to queries about processing activities.

The DPDP Rules do not provide a timeline for the Data Fiduciaries to respond to the requests. However, Data Fiduciaries and Consent Managers are required to specify timelines for responding and taking action under their grievance redressal system, which shall be published on their website and/or app. Similarly, the process for nomination may be specified in the terms of service, or as per any other applicable law. Every Data fiduciary must publish the business contact information of a person (or Data Protection Officer) in response to every request for exercise of rights by the Data Principal to respond to queries about processing activities.

REDESIGNING PRIVACY



8. Special Provisions for Children and Individuals with Disabilities

Additional safeguards are provided for processing the data of children and individuals with disabilities.

- **Verification of Parental Consent:** Data fiduciaries must implement measures to verify the authenticity of consent from parents or lawful guardians before processing a child's data. This may be through:
 - a) Reliable details based on existing account relationship with parents (age and identity), or,
 - b) Voluntarily provided details of age and identity (Government issued ID or Digital Locker Service) or a virtual token mapped to these.
- **Exemptions for Certain Entities:** Certain entities like healthcare and educational service providers can process such personal data under defined circumstances without compliance with parental consent requirements and prohibition of behavioral monitoring. This balance seeks to protect children while allowing essential services to operate effectively.
- **Exemptions for Certain Processing Purposes:** Data Fiduciaries do not need parental consent for creation of user accounts for email communication, for performing a function in the best interests of a child under law, for prohibiting access to information likely to cause detrimental effect on the well-being of a child, etc.

9. Data Retention and Erasure

Certain Data Fiduciaries (E-commerce entities with at least 2 crore registered users; Online gaming intermediaries with at least 50 lakh registered users; and Social Media intermediaries with at least 2 crore registered users) are required to adhere to three years retention timelines for personal data except for access to user account or virtual token issued by the Data Fiduciaries. If Data Principal does not engage with such data fiduciaries within the defined time period, their personal data must be erased unless legally required to retain it. Individuals must be informed 48 hours before their personal data is erased, allowing them to intervene if needed.

This provision aligns with the principles of data minimization, reducing risks associated with unnecessary data retention.

REDESIGNING PRIVACY



10. Obligations of Significant Data Fiduciaries

The DPDP Rules imposes heightened responsibilities on entities classified as Significant Data Fiduciaries based on their data processing scale or potential risks.

- **Annual DPIAs & Audits:** SDFs must conduct Annual Data Protection Impact Assessments (DPIAs) and audits to evaluate their compliance with the DPDP Rules. A report containing significant observations from the DPIAs and Audits must be submitted to the Board.
- **Algorithmic Accountability:** Algorithms (automated processing) used for data processing must be audited to ensure they do not adversely affect the rights of Data Principals.
- **Data Localization:** Certain categories of personal data and related traffic data can be subject to transfer restrictions if specified by the Central Government. This would require SDFs to ensure such data is not transferred outside Indian territory.

These measures ensure stricter compliance for entities with significant influence over large-scale data processing.

11. Cross-Border Transfer of Data

Digital personal data applicable under the DPDPA can be transferred outside the Indian territory subject to meeting conditions that may be set by the Central Government with respect to access of such data to a foreign state including any entity under the control of or agency of such State. These restrictions are applicable to all outbound transfers of personal data, whether transferred by a data fiduciary within or outside the territory of India.

12. Exemptions for Research and Archiving

The DPDP Rules exempts personal data processing for research, archival, or statistical purposes from certain obligations, provided it complies with data protection standards provided in the DPDP Rules.

13. Government Access Requests

The DPDP Rules empower the Government to request information from Data Fiduciaries for specific purposes when necessary for national security, sovereignty and integrity of the State. Disclosures of such requests cannot be made without prior written permission from the Government if such disclosure is likely to prejudicially affect the sovereignty and integrity of India or security of the State.

REDESIGNING PRIVACY



14. Functioning of the DPB and Appeals

The functioning of the Data Protection Board (DPB) is structured to ensure efficient operation as a digital office. The Board's ability to conduct proceedings electronically enhances accessibility and expedites decision making processes related to personal data protection matters. Even the appeal to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) must be filed in a digital form, emphasizing the Government's aim to implement and operationalize the Data Protection framework in a digital manner.

Conclusion

The draft DPDP Rules are a cornerstone of India's data privacy framework, offering a guide for implementing the DPDPA. The much-anticipated DPDP Rules were expected to provide clarity on the implementation of certain obligations under the DPDPA. While they address some aspects, they also leave several areas open to interpretation, creating challenges for timely implementation and compliance efforts. Given the wide-ranging implications of the DPDP Rules, it is crucial for stakeholders to actively engage in the consultation process to address these concerns effectively. Additionally, it is critical that data fiduciaries initiate their journey of compliance with the DPDPA at the earliest, which is a complex, time-consuming and resource intensive exercise.

For any query, you may reach out to **Akshay S Nanda**, Partner (Competition Law and Data Privacy Practice) at Akshayys.Nanda@sarafpartners.com.

Disclaimer: The contents of this document are provided for informational purposes only and should not be construed as legal advice on any subject matter. You should not act or refrain from acting on the basis of any content included in this document without seeking legal or other professional advice.

Contact us:

www.sarafpartners.com | [LinkedIn](#) | [X](#) | [Facebook](#) | [Instagram](#)

Our Offices:

Delhi NCR | New Delhi | Mumbai | Bengaluru | Hyderabad