09.01.2025

DSCI SUMMARY OF DRAFT DIGITAL PERSONAL DATA PROTECTION RULES 2025

On 3rd January 2025, the Ministry of Electronics and Information Technology published the Draft Digital Personal Data Protection Rules 2025 for public consultation. This document is intended to provide a high-level summary of the noteworthy details that have been introduced through the draft Rules to the data protection framework in India. It is important to note that these provisions are undergoing public consultation and will only be considered binding law after final notification in the Gazette. For detailed information on the provisions of the rules, see the official full text of the rules here.

I. Notice, Consent, and Consent Managers

Relevant provisions- Rules 3 and 4 read with the First Schedule

Summary of provisions- The rules provide that the notice to data principals should be understandable independently of any other information that has been made available. A notice should also specify the purposes of processing and contain itemized description of personal data and goods/services to be enabled by processing of personal data. On Consent Managers, Rule 4 and the First Schedule introduce conditions for registration of consent managers and their obligations. Amongst other things, this includes avoiding conflict of interest with Data Fiduciaries, incorporation of consent managers as a company in India, maintenance of consent related logs for a minimum period of seven years, etc.

II. Verifiable consent

Relevant provisions- Rules 10 and 11 read with the Fourth Schedule

Summary of provisions- For two categories of vulnerable groups, i.e. persons with disabilities and minors, the DPDP Act and draft rules require verifiable consent from the guardian or parent. The draft rules provide some detail on effectuating it by stating that upon the declaration by a child or upon the parent approaching the Data Fiduciary, the Data Fiduciary shall have the responsibility to verify the age and identity details of the person identifying themselves as the parent. This may be done through virtual tokens, digital locker service providers, or entities entrusted under the law. There are some exemptions from this requirement for educational and healthcare institutions as well as for processing which is in the best interest of the child or for the safety of the child.

III. Reasonable security safeguards and data breach reporting

Relevant provisions- Rules 6 and 7

Summary of provisions- Rule 6 provides a list of minimum reasonable security safeguards to be implemented by all Data Fiduciaries including encryption and masking of personal data, implementing access control, log monitoring and review, instituting data backups for continued processing in the event of a compromise, retention of logs, provisioning for contractual safeguards between Data Fiduciaries and Processors, and ensuring effective observance of security safeguards. Under Rule 7, any personal data breach must be intimated to both Data Principals and to the Data Protection Board. To the Data Protection Board, a description of the breach must be intimated without delay and a more detailed report has to be furnished within 72 hours of becoming aware of the breach.

IV. Data retention limitation

Relevant provisions- Rule 8 and the Third Schedule

Summary of provisions- Rule 8 and the Third Schedule provide for defined periods of data retention for three classes of Data Fiduciaries- e-commerce, social media, and online gaming. In cases of inactivity from the Data Principal for a period of three years, personal data of such Data Principals is required to be erased except such data which is required to ensure access to user account or any virtual tokens. Additionally, before such erasure of personal data is undertaken, Data Fiduciaries are required to provide a 48-hour prior intimation to the individuals.

V. Additional obligations for significant data fiduciaries

Relevant provision- Rule 12

Summary of provision- Additional obligations for Significant Data Fiduciaries ('SDF') include conducting annual data protection impact assessments and audits and submission of reports containing significant findings to the Data Protection Board. Any algorithmic software deployed by SDFs for modification, transmission, storage, etc. of personal data would require due diligence from the SDF to assess any risks to rights of Data Principals. Finally, personal data specified by the Central Government and traffic data pertaining to its flow would be restricted from being transferred outside India by the SDF.

VI. Restrictions on personal data being made available to foreign state

Relevant provision- Rule 14

Summary of provision- The provision states that when personal data is being processed to offer goods or services to Data Principals within the territory of India, whether that data is processed within or outside India, such processing will be subject to requirements specified by the Central Government on making such personal data available to any foreign State, or person/entity under the control of such foreign State.

VII. Establishment of the Data Protection Board

Relevant provisions- Rules 16 to 21 and Fifth and Sixth Schedule

Summary of provisions- These provisions provide for the procedural and operational aspects related to the establishment and functioning of the Data Protection Board. This includes the appointment of the chairperson and members of the Board, prescription of a six-month timeline for completion of inquiries, the digital by design functioning of the Board, procedure for filing appeals, etc.

VIII. Power to call for information

Relevant provisions- Rule 22 and Seventh Schedule

Summary of provisions- The rule and corresponding Seventh Schedule empower the Central Government to call for such information, including personal data of data principals, from data fiduciaries and intermediaries which is necessary in the interest of sovereignty and integrity, or security of the State, for performance of any legal function by the State or its instrumentalities, or for carrying out an assessment for notifying which data fiduciaries qualify as SDFs.