DPDP: The Fine Print

The notification of the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") this month has given shape to a definite compliance regime under the aegis of Digital Personal Data Protection Act, 2023 ("**DPDP Act**").

A reading of the DPDP Rules will quickly validate the view that companies are expected to demonstrate accountability, when it comes to Personal Data[1], and the burden of compliance and proof (in most cases) is on the Data Fiduciary[2]. So far, data privacy laws in India have been scattered, with the major sector-agnostic law being the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which was limited in terms of catering to the changes in the business landscape.

Considering that implementation at this scale is going to require time, money and effort, the compliance timeline under the DPDP Rules has been phased out. For businesses, the real work begins now. The DPDP Rules will require businesses to look closer at the nature of data collected, the processes followed and ensure that appropriate technologies and systems exist around consent collection, data retention, breach protocols, etc.

In this article, we examine how the key provisions of the DPDP Rules reshape operational and legal responsibilities, where the compliance burden is highest, and what businesses should prioritize in the coming months. The provisions we have analyzed in the table below come into effect 18 months from the date of notification in the Gazette, being May 2027.

Heading	Compliance	Implication
Data Fiduciary Obligations		
Notice ***(Rule 3)*** 	Notice given by the Data Fiduciary to the Data Principal[3] to obtain consent for collecting their Personal Data shall: (i) be presented and be understandable independently of any other information; (ii) give, in clear and plain language, a fair account of the	(i) Companies will need to reconsider the manner in which the notice document / privacy policy is worded. In other words, notices cannot be tucked away discreetly in long-wound, difficult to understand terms and conditions.

[1] Any data about an individual who is identifiable by or in relation to such data.
[2] Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
[3] The individual to whom the personal data relates and where such individual is: (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.

Heading	Compliance	Implication
	details necessary to enable the Data Principal to give specific and informed consent for the processing of her Personal Data; (iii) give the communication link for accessing the website or app, or both, of such Data Fiduciary for withdrawing her consent, exercising her rights and making a complaint to the Board[4].	(ii) An itemized description of all Personal Data should map each item of Personal Data being collected against the purpose for which such data is proposed to be used. In other words, a generic language of 'providing goods and services' may no longer stand the test of law. (iii) Withdrawal of consent will need to be as easy for the Data Principal as it was for providing consent (which could mean, a similar click button). (iv) Considering the above, businesses will also need to build a system in place where a record of all of the above is maintained on a case-to-case basis, in case they need to demonstrate compliance with the DPDP Rules.
Verifiable Consent **(*Rules 10 and 11*)** 	(i) Children: The Data Fiduciary will adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any Personal Data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable. (ii) Disabled person with lawful guardian: A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such	The two major implications of the verifiable consent requirement, is that Data Fiduciaries will need to build technical infrastructure to ensure that the consent obtained from the parent / guardian is verifiable. In other words, a mere 'Click OK' button or warranties from the user will not be sufficient. The other legal implication is that the burden of proof is on the Data Fiduciary to show that due consent was obtained. This means added compliance cost, redesign of onboarding flows, and maintaining audit-ready proof of consent for children and persons with disabilities

[4] Data Protection Board of India established under the DPDP Act.

Heading	Compliance	Implication
	guardian is appointed by a court of law, or by a designated authority or by a local level committee, under the law applicable to guardianship.	(which will include an understanding of guardianship laws).
Time period for retention of data (*Rule 8*) 	As a thumb rule, a Data Fiduciary is required to retain data (including traffic data and other logs) for at least 1 year from the date of processing of such data. In cases of certain specific Data Fiduciaries (like e-commerce companies, online gaming intermediary and social media intermediary)[5], Data Fiduciaries are required to retain data for a period of 3 years from the last usage by the Data Principal for the specified purpose or exercise of rights. Further, where a Data Fiduciary has engaged a Data Processor[6] for the processing of data, it is the obligation of the Data Fiduciary to ensure that the Data Processor also retains the data for the above time periods.	Businesses will need to build systems that track user activity (last login, last rights exercise) to know when the "specified purpose" is no longer being served. To comply efficiently, businesses may need automated data deletion pipelines that can identify which users' data is eligible for erasure, trigger the 48-hour notification, and then carry out erasure if there's no response. Unless automated, this may result in significant costs in terms of resources and also increase the scope for human error.
Contact information (*Rule 9*) 	Every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the DPDP Act, the business contact information of the Data Protection Officer[7], if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions of the	Companies must designate a person who understands data protection well and sending of a generic "support" email may not work.

[5] E-commerce entity having not less than two crore registered users in India, online gaming intermediary having not less than fifty lakh registered users in India and a social media intermediary having not less than two crore registered users in India.
[6] Any person who processes personal data on behalf of a Data Fiduciary.
[7] Only required to be appointed by Significant Data Fiduciaries.

Heading	Compliance	Implication
	Data Principal about the processing of her Personal Data.	
Significant Data Fiduciary[8] **(*Rule 13*)** 	The DPDP Rules impose certain additional obligations on Significant Data Fiduciaries: (a) Data Protection Impact Assessment and audit to be undertaken annually; (b) Report to be submitted to the Board; (c) Due diligence on any algorithmic software they use for data processing; (d) Data localization restrictions with respect to personal data as may be specified by the Central Government.	The Central Government has not yet notified who the Significant Data Fiduciaries will be under Section 10 of the DPDP Act. Once identified, such businesses will need to analyse costs in relation to audit, inspections, external experts, due diligence requirements, etc.
Intimation of personal data breach[9] **(*Rule 7*)** 	On becoming aware of any Personal Data breach, the Data Fiduciary is required to immediately notify the concerned Data Principal and also the Board. The notification must include nature of breach, extent, timing, location, possible consequences, mitigation measures, and what users themselves can do to protect themselves.	Data Fiduciaries will need to have processes in place to detect a breach and also analyse the nature of consequences that can arise on account of the same and have systems in place to be able to mitigate the same at the earliest. This is likely to require costs in terms of infrastructure and training since businesses will need to maintain forensic readiness: logs, access records, root cause analysis, and records of mitigation.
Security Safeguards		
Reasonable security safeguards (*Rule 6*) 	Data Fiduciaries are required to have the following safeguards as a minimum with respect to Personal Data in its possession or control and also in respect of any processing done by a Data Processor: (a) encryption, obfuscation, masking or the use of virtual	Businesses will require to revisit their infrastructure and security systems to ensure the standards in Rule 6 are met, which are not merely 'good to have' standards but more of a bare minimum requirement. Businesses will need to build or improve encryption, ensure access to

[8] Any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10. This has not been notified yet.
[9] Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

Heading	Compliance	Implication
	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) data back-ups in case of data being compromised; (e) retention of data and its logs for 1 year; and (f) ensure contractual safeguards in the contracts entered into with the Data Processor.	Personal Data in the organization is given on a need basis, and put in place a good monitoring system to ensure that breaches are identified promptly. Further, considering Data Fiduciaries are responsible for breaches by Data Processors, Data Fiduciaries will need to ensure adequate contractual safeguards to ensure Data Processors' compliance and also seek audit and access rights to the systems of Data Processors.
Data Principal Rights		
Rights of Data Principals (*Rule 14*) 	Data Fiduciary and Consent Manager[10] are required to publish the details of the means using which a Data Principal may make a request for the exercise of rights. All grievances will need to be responded to within 90 days.	Businesses must invest in systems, training and adherence to grievance timelines to ensure that the rights of Data Principals are honored.
Data Localization		
Transfer of personal data outside the territory of India (*Rule 15*) 	Any Personal Data processed by a Data Fiduciary under the DPDP Act may be transferred outside the territory of India subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such Personal Data available to any foreign State, or to any person	No order has yet been made by the Central Government regarding transfer of Personal Data outside India. This will be key for cross-border businesses that use personal data of customers across different jurisdictions, since this is not just a question of compliance cost but also viability of business models.

[10] A person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform

Heading	Compliance	Implication
	or entity under the control of or any agency of such a State.	
Governments' use of Personal Data		
Processing of personal data for State and its instrumentalities (*Rule 5*) 	The State and its instrumentalities are permitted to process Personal Data of Data Principals for provision or issue of subsidy, benefit, service, certificate, license or permit. Such processing has to be done (a) in a lawful manner; (b) while limiting the use of such Personal Data as is required to achieve the purposes; and (c) maintaining reasonable security practices.	In this case, the DPDP Rules treat the Government arm as a Data Fiduciary and makes them subject to largely similar obligations as a private business. However, it is interesting to note that the Government arm will not be subject to the obligations of Data Fiduciaries in the context of 'obtaining consent'. If the Government arm engages a private company for such compliance, the private company will be bound by obligations in the capacity of a Data Processor.
Obligation to disclose to the Central Government (*Rule 23*) 	The Central Government has the right to call upon any Data Fiduciary or intermediary to furnish information regarding Data Principals for the following purposes: (a) Use of Personal Data of a Data Principal in the interest of sovereignty and integrity of India or security of the State; (b) Use of Personal Data of a Data Principal for the performance of any function under any law for the time being in force in India or disclosure of any information for fulfilling any obligation under any law for the time being in force in India; and (c) Carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.	Authorised persons have been specified for each of the purposes for which the Central Government may seek access to Personal Data of Data Principals. Further, the Central Government may also require the Data Fiduciary or intermediary to not disclose the furnishing of such information to the concerned Data Principal, if the information of such furnishing is likely to prejudicially affect the sovereignty and integrity of India or security of the State. Considering the scope of purpose for which the Central Government may seek information is broad and the Central Government is also empowered to require the Data Fiduciary to not notify the Data Principal that their Personal Data has been shared, it may limit the ability

Heading	Compliance	Implication
		of Data Principals to seek remedies in case of disclosure of their Personal Data to the Central Government.

The DPDP Act, now read with the DPDP Rules, is a step in the right direction to build some sort of legal discipline in the data privacy regime. The 18-month time period given before the key compliances kick-in, with the Board already in the process of being set up, will give businesses the much-needed time to be operationally ready for compliance.

Authors:

Pradeep Reddy | Hitesh Mallick | Saumya Ramakrishnan

Contact: saumya@bombaylawchambers.com