FoxMandal
Solicitors & Advocates

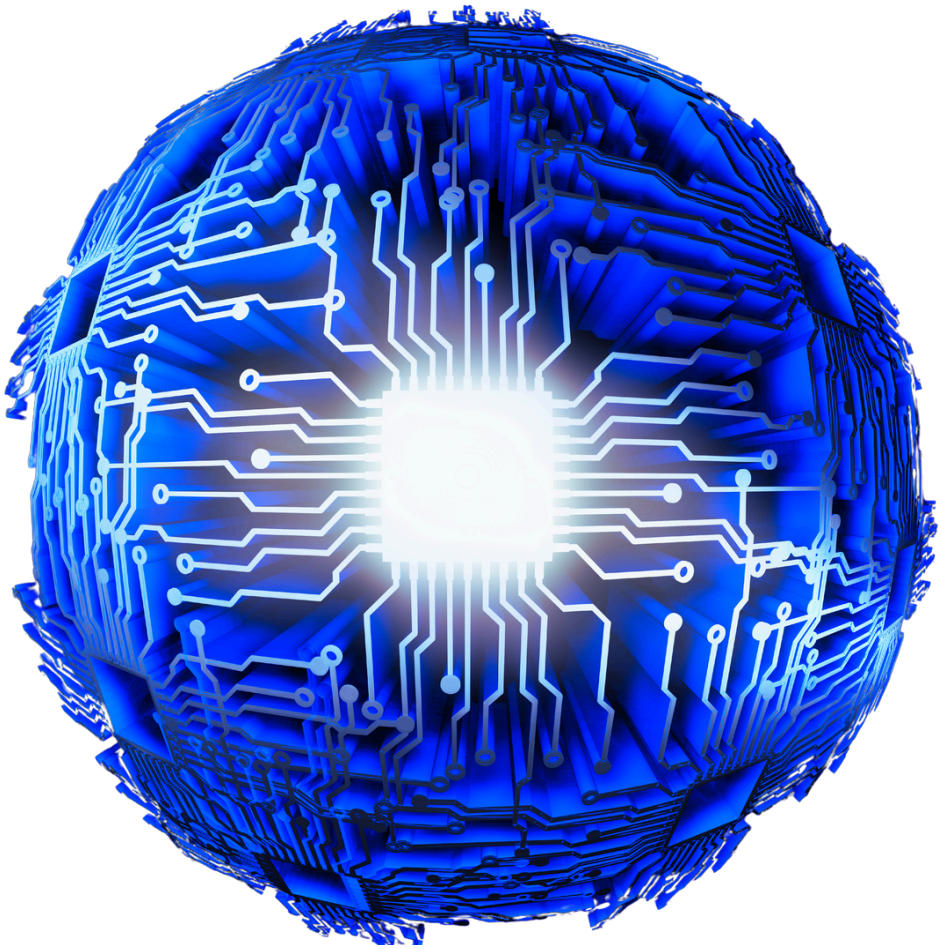


FAQs

10 Essential Questions on the Draft DPDP Rules, 2025

January 28, 2025

FoxMandal
Solicitors & Advocates

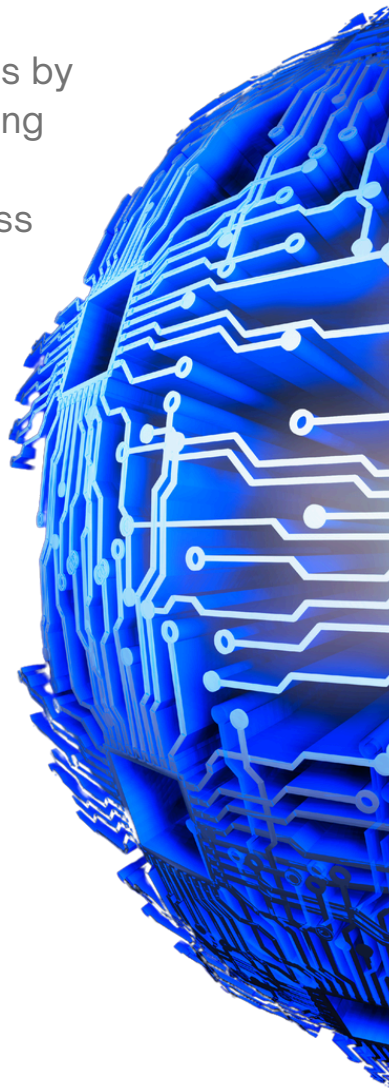


Since its introduction in August 2023, the Digital Personal Data Protection Act, 2023 ("DPDP Act"), along with the draft DPDP Rules, 2025 ("Draft Rules"), released earlier this month, has prompted extensive dialogue. Understanding the practical implications and compliance requirements the Draft Rules seek to introduce is essential before their finalization to ensure smooth implementation.

In this FAQ, we address some of the key questions organisations may have as they navigate the changes and prepare for effective rollout of the Act and the Rules.

1. How can DPDP compliance be integrated into a data fiduciary's data practices?

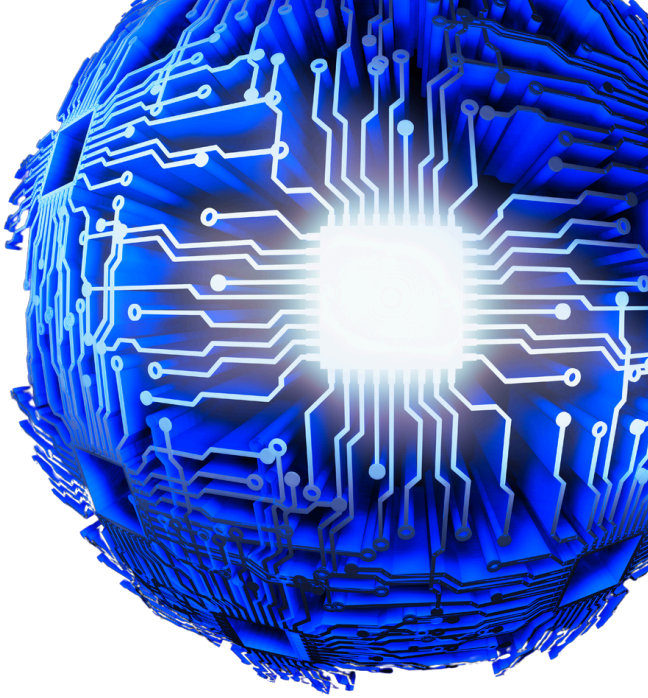
Embed privacy and data protection into your core operations by ensuring transparency in data processing practices and taking reasonable security safeguards to prevent personal data breaches. Set up a cross-functional team to ensure seamless compliance with both legal and operational aspects of data protection.



2. How should data fiduciaries handle data retention and erasure?

E-commerce entities, online gaming intermediaries, and social media intermediaries having a significant user base, as specified, must erase personal data after three years from the date on which the data principal last approached the data fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the DPDP Rules, whichever is later. This ensures that data is retained only when: a) the entity processes personal data for the purpose of enabling the data principal to access their user account or virtual tokens, or b) for ensuring compliance with the law.

For other classes of data fiduciaries, personal data must be erased upon: a) consent withdrawal, or b) as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier. Such data may only be retained for compliance with the law.



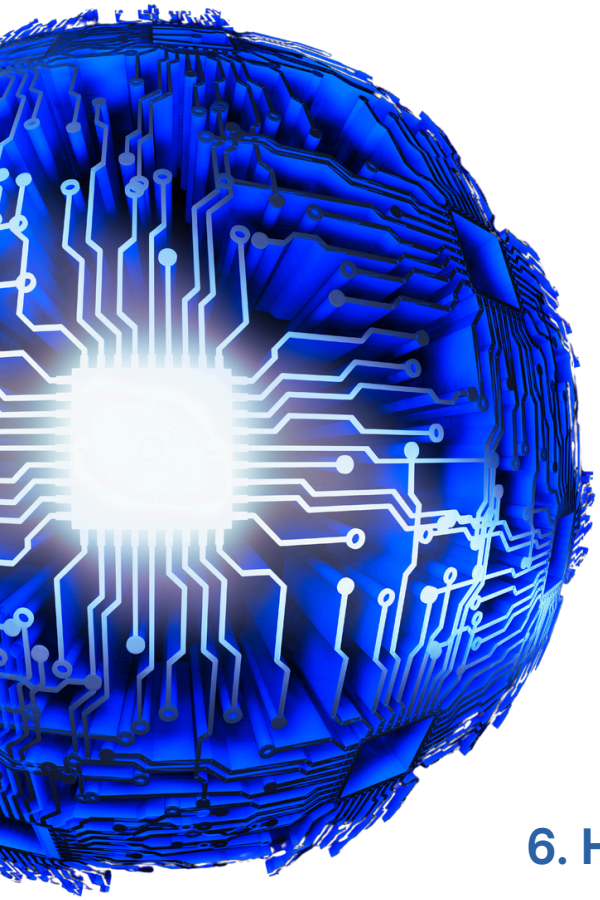
3. Is it mandatory for data fiduciaries to ascertain if the data principal is a child?

Additional measures for processing children's personal data encompass securing verifiable parental consent and observing due diligence requirements to verify the age and identity of the parent or lawful guardian. However, there is no provision mandating data fiduciaries to ascertain if the data principal is a child. Having said that, the Draft Rules allow data fiduciaries to seek confirmation that the data principal is not a child, by undertaking tracking or behavioural monitoring of the child, etc.

4. What is the way forward in cases where consent was obtained prior to the commencement of the DPDP Act?

If consent for processing personal data was provided prior to the commencement of the Act, the required notice has to be given "as soon as it is reasonably practicable" and in the manner as may be specified by the Central Government. Such processing can continue until the consent is withdrawn. It is recommended to audit existing data to identify where consent was given before the commencement of the Act. Use email, app notifications, or public announcements to notify users, and set a clear timeline to complete this process.

5. What new requirements do data processors have to comply with?



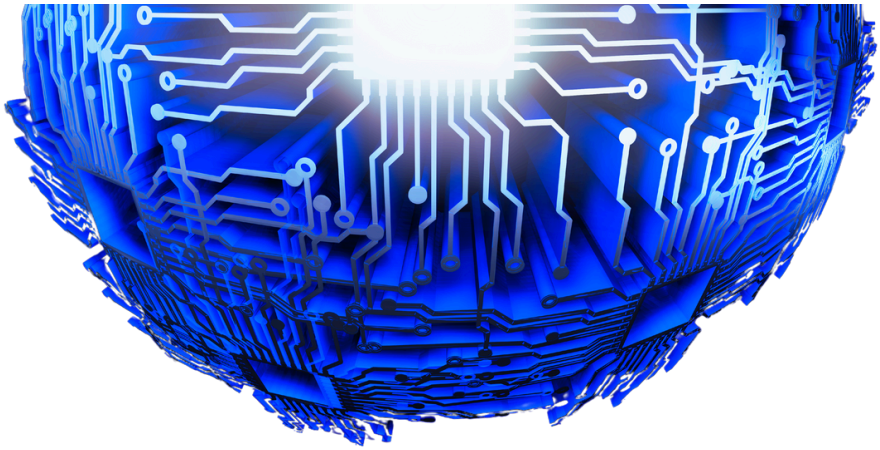
Though the Draft Rules specify that contracts executed with data processors should include provisions for taking reasonable security safeguards, the same is taken to mean that the contract will enable data fiduciaries to ensure that security measures are in place. The Act mandates the existence of a valid contract between the data fiduciary and the data processor for the processing of personal data on behalf of the fiduciary. Essentially all obligations of the data fiduciary are contractually transferred to data processor. In view of this, it is advisable to adopt best practices and align your safeguards with industry standards.

6. How can data fiduciaries prepare for cross-border data transfer restrictions?

Cross-border data transfers will be subject to the requirements specified by the Central Government. Further, data localisation obligations require Significant Data Fiduciaries (SDFs) to adopt measures to ensure that the personal data specified by the Central Government (and the traffic data pertaining to its flow) is not transferred outside of India. Before these restrictions take effect, it would be prudent to review your data flows to identify any cross-border transfers that may be impacted. Also, build flexible systems that can comply with both local and international regulations.

7. What should SDFs do for Data Protection Impact Assessments and algorithm checks?

Significant Data Fiduciaries (SDFs) must undertake annual Data Protection Impact Assessments (DPIAs) and audits, and conduct due diligence to verify that any algorithmic software they use to process personal data does not pose a risk to the rights of data principals. Automated tools may be used for risk evaluations, and legal and IT teams could be involved to assess the fairness and transparency of algorithms.



8. How can consent managers be leveraged to improve customer experience and ensure compliance?

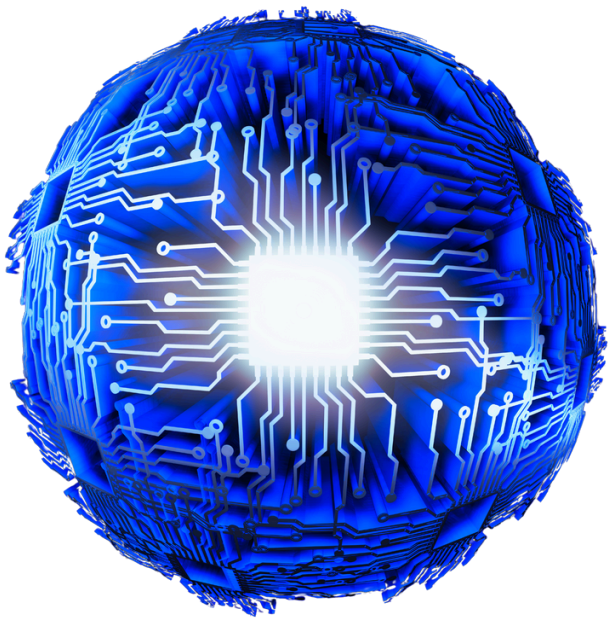
Consent managers need to have a certified interoperable platform allowing users to give, manage, review and withdraw their consent to the processing of their personal data. Leverage consent managers to simplify the consent process with an easy-to-use, transparent interface. Also, ensure the platform integrates smoothly with the system and is in line with the prescribed data protection standards and assurance framework.

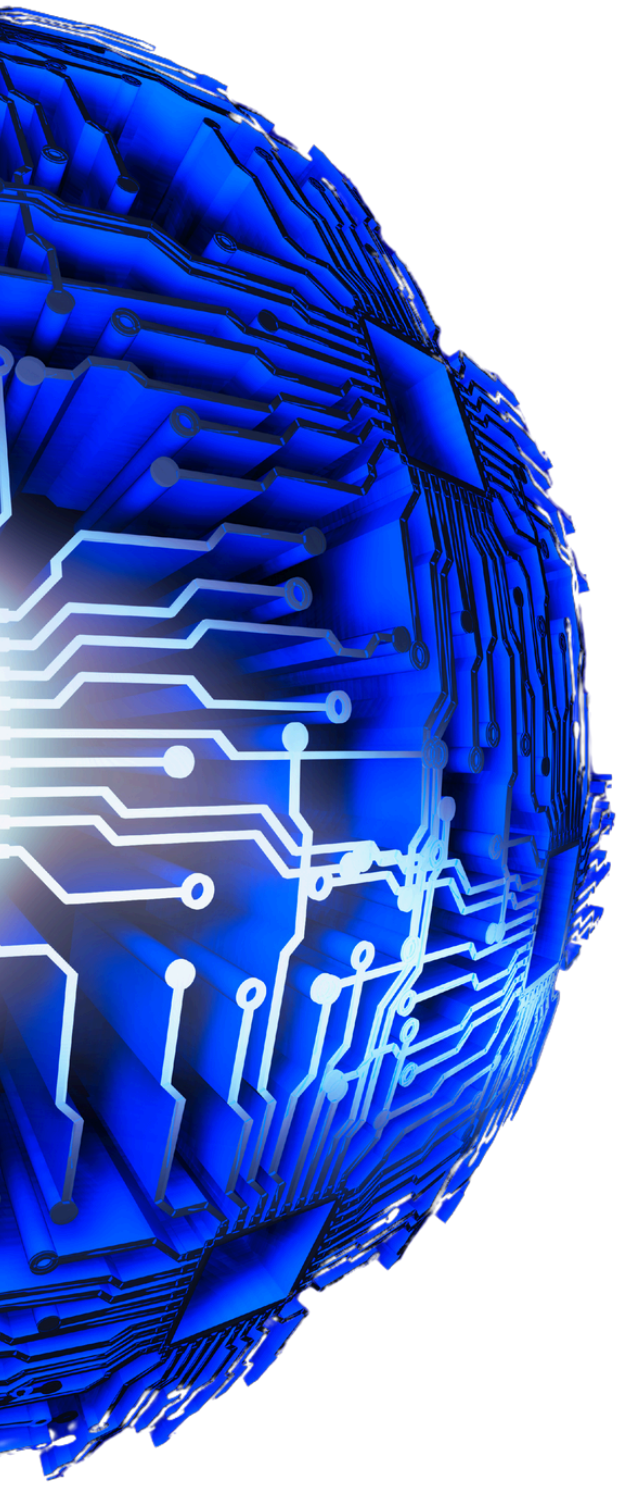
9. How should data fiduciaries handle breach notifications to reduce business risks?

Data fiduciaries should have a response plan in place, train their team to act quickly, and follow clear processes for investigating, reporting, and communicating breaches within the prescribed timelines. Running breach simulation exercises would help with preparedness.

10. What penalties are applicable for non-compliance, and how can organisations avoid them?

Non-compliance could lead to penalties of up to INR 250 crores. To avoid penalties, ensure compliance through regular risk assessments, employee training, and privacy by design practices. Seeking external advice can further reduce compliance risks.





The Draft Rules strike a delicate balance between safeguarding personal data and offering organisations latitude to manage their operations effectively.

By integrating privacy into core operations, adhering to data retention and erasure protocols, and implementing appropriate measures, businesses can not only mitigate risks but also build stronger trust with their users.

Proactive actions, such as conducting regular audits and employee training, will help avoid penalties and ensure that data protection remains at the forefront of business practices.

The Draft Rules are likely to be modified or amended following ongoing government consultations.

For further queries, you may reach out to our Technology Team at info@foxmandal.in