FREQUENTLY ASKED QUESTIONS: DIGITAL PERSONAL DATA PROTECTION FRAMEWORK [DPDP ACT, 2023 AND DPDP RULES 2025]

THEME: DATA FIDUCIARY AND SIGNIFICANT DATA FIDUCIARY

Question	Answer	Relevant Section of DPDP Act, 2023	Relevant Section of DPDP Rules, 2025
Who is a "Data Fiduciary"?	A Data Fiduciary is any person (including individuals, companies, or the State) who, alone or in conjunction with others, determines the purpose and means of processing personal data.	Section 2(i)	-
What are the general obligations of a Data Fiduciary?	The Data Fiduciary is responsible for compliance with the Act for any processing undertaken by it or on its behalf by a Data Processor. It must ensure data completeness, accuracy, and consistency if the data is used to make decisions affecting the individual or is shared with another Fiduciary.	Section 8(1), 8(2), 8(3)	-
What security measures must a Data Fiduciary implement?	Fiduciaries must take reasonable security safeguards to prevent personal data breaches. This includes encryption, obfuscation, masking, or using virtual tokens; controlling access to computer resources; and maintaining logs and monitoring to detect unauthorized access.	Section 8(5)	Rule 6
What is the procedure for a	In the event of a breach, the Fiduciary must intimate the Board and each affected Data Principal. The intimation to the	Section 8(6)	Rule 7

Personal Data Breach (PDB)?	Principal must include a description of the breach, likely consequences, and safety measures they can take.		
What information must a Data Fiduciary provide to affected individuals (Data Principals) after a breach?	The Data Fiduciary must, to the best of its knowledge, intimate each affected individual in a concise, clear, and plain manner without delay. The notice must include: 1. A description of the breach (nature, extent, and timing); 2. Likely consequences for that specific individual; 3. Mitigation measures implemented or being implemented by the Fiduciary; 4. Safety measures the individual can take to protect her interests; 5. Business contact information of a person authorised to respond to queries.	Section 8(6)	Rule 7(1)
What detailed information must be submitted to the Board in the follow-up report?	Within seventy-two hours of becoming aware of the breach (or a longer period if allowed by the Board in writing), the Fiduciary must provide: 1. Updated and detailed information regarding the initial description; 2. Broad facts related to the events, circumstances, and reasons for the breach; 3. Mitigation measures implemented or proposed; 4. Any findings regarding the person who caused the breach; 5. Remedial measures taken to prevent recurrence; 6. A report regarding the intimations already given to affected individuals.	Section 8(6)	Rule 7(2)
How can individuals contact the Data Fiduciary	Every Data Fiduciary must prominently publish business contact information for a Data Protection Officer (DPO) or a person capable of answering questions about data processing.	Section 8(9)	Rule 9

regarding their data?			
How is an organization identified and notified as an SDF?	The Central Government notifies an SDF based on factors like the volume and sensitivity of personal data, risk to Data Principal rights, potential impact on sovereignty and integrity of India, or security of the State.	Section 10(1)	
What are the specific accountability requirements for the DPO appointed by SDF?	The DPO must be based in India, represent the SDF under the Act, be responsible to the Board of Directors (or similar governing body), and serve as the primary point of contact for the grievance redressal mechanism.	Section 10(2)(a)	
How often must an SDF conduct audits?	An SDF must undertake a DPIA and an audit once every twelve months and submit a report with significant observations to the Board.	-	Rule 13(1), 13(2)
What is "algorithmic due diligence" for an SDF?	An SDF must verify that its algorithmic software used for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing data is not likely to pose a risk to the rights of Data Principals.	-	Rule 13(3)
What are the reporting obligations regarding DPIAs and audits?	An SDF must cause the person carrying out the DPIA and audit to furnish a report to the Data Protection Board (the Board). This report must contain all significant observations made during the assessment and audit process.	Section 10(2)(c)	Rule 13(2)
What is the timeframe for an SDF to complete	An SDF must undertake both a DPIA and an audit once in every period of twelve months from the date it is notified or included in the notified class of SDFs.	-	Rule 13(1)

its mandatory assessments?			
Are there specific cross-border restrictions for SDFs?	Yes. Based on the recommendations of a committee constituted by the Central Government, an SDF must ensure that specified personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.	-	Rule 13(4)
Who makes the recommendations regarding SDF data transfer restrictions?	Recommendations are made by a committee constituted by the Central Government, which includes officials from MeitY and may include officials from other Ministries or Departments of the Central Government.	-	Rule 13(4) Rule 13(5)