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

THEME: REASONABLE SECURITY SAFEGUARDS

S. No.	Questions	Answers
1.	What are "reasonable security safeguards", and what specific measures do they entail?	Under the Act, a Data Fiduciary is mandated to protect personal data in its possession or control by taking reasonable security safeguards specifically designed to prevent a "personal data breach". A breach is defined as any unauthorised processing or accidental event - such as disclosure, alteration, or destruction - that compromises the confidentiality, integrity, or availability of personal data. According to the notified Rules, these safeguards are not merely discretionary but must include, at a minimum, the following detailed technical and organisational measures: • **Data Security Protocols:** Protecting data with encryption, obfuscation, masking, or virtual tokens mapped to the personal data. • **Access Management:** Implementing robust measures to control access to the computer resources used by the Data Fiduciary or Data Processor. • **Monitoring and Visibility:** Maintaining logs, monitoring, and periodic reviews to ensure visibility into who is accessing data, enabling the detection and investigation of unauthorised access. • **Business Continuity and Recovery**: Establishing measures for continued processing if data is destroyed or access is lost, such as maintaining regular data-backups. • **Mandatory Log Retention:** To facilitate the investigation of breaches and remediation, Fiduciaries must retain processing logs and personal data for a period of one year, unless a different period is required by another law.

		• **Contractual Enforcement:** Ensuring that the contract between a Data Fiduciary and a Data Processor contains explicit provisions requiring the Processor to uphold these security safeguards. • **Effectiveness Assurance**: Adopting overarching technical and organisational measures to verify that all implemented security safeguards are functioning effectively.
2.	What is the fundamental obligation regarding data security?	Every Data Fiduciary is legally required to protect personal data in its possession or under its control. This includes protection against personal data breaches by implementing reasonable security safeguards. This obligation applies to all processing, whether undertaken by the Data Fiduciary itself or by a Data Processor on its behalf. • *Relevant Provision*: **Section 8(5)** of the Act; **Rule 6(1)** of the Rules.
3.	Does the Data Fiduciary remain responsible for security if they use a Data Processor?	Yes. A Data Fiduciary is responsible for complying with the Act for any processing undertaken on its behalf by a Data Processor. The Data Fiduciary may only engage a Data Processor under a valid contract. Furthermore, the Rules mandate that this contract must include appropriate provisions ensuring the Data Processor takes reasonable security safeguards. • *Relevant Provision:* **Sections 8(1)** and **8(2)** of the Act; **Rule 6(1)(f)** of the Rules.
4.	What are the "minimum" security measures required by law?	The Rules specify that reasonable security safeguards must include, at a minimum, the following technical and organisational measures: • Data Security • Access Control • Visibility and Monitoring • Business Continuity • *Relevant Provision:* **Rule 6(1)(a), (b), (c), (d),** and **(g) of the Rules.**

5.	Is there a mandatory period for retaining security logs?	Yes. For the purposes of detecting, investigating, and remediating unauthorised access, Data Fiduciaries must retain logs and the associated personal data for a period of one year. This retention is required unless compliance with another law currently in force necessitates a different period. • *Relevant Provision:* **Rule 6(1)(e)** of the Rules.
6.	Are there specific standards for State instrumentalities?	When the State or its instrumentalities process personal data to provide subsidies, benefits, or services, they must follow the standards specified in the Second Schedule. This includes taking reasonable security safeguards to prevent breaches for any processing they perform or that is performed on their behalf by a Data Processor. • *Relevant Provision*: Rule 5(1) of the Rules; Item (f) of the Second Schedule.
7.	What is the penalty for failing to implement reasonable security safeguards?	Failure to observe the obligation to take reasonable security safeguards to prevent a personal data breach is a significant breach. Under the Act, the Data Protection Board of India may impose a monetary penalty for this specific failure that may extend to **two hundred and fifty crore rupees (₹250 crore).** • *Relevant Provision*: **Section 33** of the Act; **Sl. No. 1** of The Schedule.
8.	What are the requirements for business continuity and data availability?	The DF must have reasonable measures for continued processing if the confidentiality, integrity, or availability of personal data is compromised (e.g., due to destruction or loss of access). This includes measures such as data backups. • *Reference:* Rule 6(1)(d) of the Rules.