Science & Technology · GS - III

Examine the challenges of ensuring personal data protection in an economy increasingly dependent on third-party digital service providers.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 28/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

DPDP Act 2023, Data Fiduciary, Data Processor, third-party vendors, data breach, accountability, cybersecurity, digital governance

Model Answer

India's expanding digital economy increasingly relies on cloud services, payment platforms, analytics providers and outsourced technology vendors. While these services improve operational efficiency, they also create vulnerabilities in personal data protection.

The Digital Personal Data Protection (DPDP) Act, 2023 establishes a framework for regulating the processing of digital personal data and strengthening accountability.

Key challenges associated with third-party data processing include:

1. **Accountability gaps:** Outsourcing data processing can create confusion regarding responsibility when vendors fail to maintain adequate safeguards.
2. **Cybersecurity vulnerabilities:** Weak encryption, inadequate access controls and insecure storage systems increase the risk of breaches.
3. **Supply-chain complexity:** Organisations may lack visibility over subcontractors and the movement of personal data across systems.

4. **Data retention risks:** Inadequate deletion mechanisms can result in unnecessary storage and unauthorised access.
5. **Regulatory compliance:** Organisations must ensure that contractual arrangements and operational practices meet applicable legal obligations.

The DPDP framework places statutory responsibilities on Data Fiduciaries, including when they engage Data Processors. This makes vendor due diligence an essential component of organisational compliance.

A robust response requires periodic security audits, clear contractual responsibilities, restricted access privileges, encryption, incident-response protocols and verified data-deletion procedures. Employee training and independent assessments should complement these measures.

India must also strengthen institutional capacity for monitoring compliance and addressing emerging technological risks.

Ultimately, personal data protection cannot be confined to an organisation's internal systems; it must extend across the entire digital supply chain.

BECOME IAS
AI POWERED UPSC PREP