Protecting personal data in Indian MSMEs and startups

News & Updates • July 8, 2026

'First published on India Business Law Journal'

By: Shantanu Sahay and Pratyush Acharya

Data protection has become a critical part of business operations because it is not only a legal requirement under India's evolving privacy framework, but also a business control issue affecting the confidence of clients, vendors and employees.

While large corporations can afford dedicated compliance teams, micro, small and medium-sized enterprises (MSMEs) and startups often struggle with managing personal data. However, data protection for smaller businesses does not necessarily require a complex compliance structure. It requires an understanding of what personal data is collected, why it is collected, where it is stored, who can access it, how long it is retained, and how it will be protected if something goes wrong.

For most MSMEs, the current enforceable framework still comes from the Information Technology (IT) Act, 2000, the Sensitive Personal Data or Information (SPDI) Rules, 2011, and the Indian Computer Emergency Response Team's (CERT-In) 2022 cyber incident reporting directions.

Act on DPDP compliance before 2027

Although the Digital Personal Data Protection (DPDP) Act, 2023 has been enacted and draft rules have been notified, the main compliance obligations are expected to become operational only after phased implementation, likely around May 2027. Businesses should not wait for the DPDP Act to become fully operational before taking action.

Under the IT Act and SPDI Rules, businesses handling sensitive personal data are expected to implement reasonable security practices and privacy safeguards. Section 43A of the IT Act creates compensation liability where negligence in implementing reasonable security practices causes wrongful loss or gain. Section 72A penalises disclosure of personal information in breach of a lawful contract.

The SPDI Rules require businesses to maintain a privacy policy, obtain consent for collection of sensitive personal data, collect information only for lawful purposes, retain data only as long as

necessary, provide correction rights, regulate disclosure and transfer of information, and appoint a grievance officer.

Map data, controls for DPDP readiness

In practical terms, every business should be able to answer a few basic questions: what personal data it collects; why it collects it; who has access to it; where it is stored; how long it is retained; and what security controls protect it. If a business cannot answer these questions clearly, its data-protection programme is likely weak. The DPDP Act represents India's future privacy operating model. The act introduces the concepts of data fiduciary and data processor. A data fiduciary determines the purpose and means of processing personal data, while a data processor handles data on behalf of the data fiduciary.

Under the DPDP framework, businesses will need to process personal data only for lawful purposes, rely on consent or other permitted uses, provide clear notices, implement safeguards, erase data when the purpose is completed unless retention is legally required and establish grievance mechanisms.

The act also requires personal data breach notifications to the Data Protection Board and affected individuals. Significant data fiduciaries will face additional obligations such as appointing a data protection officer, conducting independent audits, and carrying out data protection impact assessments (DPIA). Most MSMEs should still adopt a risk-based approach.

Prepare for India privacy penalties

Certain sectors are subject to additional regulatory requirements. Fintech companies, insurers, brokers, exchanges and other regulated entities may face stricter obligations from regulators such as the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI) and Securities and Exchange Board of India (SEBI). The RBI's IT governance and outsourcing directions impose governance and risk management obligations, while the IRDAI and SEBI have separate cybersecurity frameworks for regulated entities.

The penalty landscape is becoming more serious. Under the current framework, negligent failure to protect sensitive personal data can result in compensation liability under section 43A of the IT Act, while unlawful disclosure may attract penalties under section 72A.

Once the DPDP Act's substantive penalty regime becomes operational, penalties may increase significantly, including up to INR2.5 billion (USD25.8 million) for failure to implement reasonable

security safeguards, and up to INR2 billion for failure to notify a personal data breach.

In conclusion, while MSMEs may face lighter compliance obligations, management of personal data is essential for every business. Privacy and cybersecurity practices are important for maintaining trust, credibility and business growth.

KEY CONTACT

Shantanu Sahay

Partner

View Bio of Shantanu Sahay