INDIALAW

Data Protection and Privacy

Data Protection and Privacy Law Firm in India for DPDP and GDPR Compliance

PRACTICE PROFILE • MAY 2026

Overview

The increasing complexity of global data regulations requires businesses to take proactive steps in protecting personal and sensitive data. Our team assists clients across sectors in developing robust data protection strategies, aligned with both domestic and international frameworks such as the Indian DPDP Act, GDPR, and other jurisdiction-specific laws. We work closely with clients to ensure lawful data collection, processing, storage, and transfer practices while mitigating enforcement risks.

Our Services

- India DPDP Act, GDPR, CCPA, HIPAA and global privacy compliance like Singapore, UAE, KSA and more.
- Data Protection Officer services to carry out day to Data Protection activities and responsibilities
- Drafting and reviewing privacy policies and consent mechanisms
- Advising on cross-border data transfers and adequacy mechanisms
- Conducting privacy impact and risk assessments
- Representation in data breach investigations and regulatory inquiries
- Data processing and sharing agreements
- Advising on data subject rights and internal governance
- Privacy audits and compliance training

Key Professionals

Appurv Bhatia

Head- Data Protection & Security

Frequently Asked Questions

Q1 **What does a data protection and privacy practice cover in India?**

It covers advising businesses on lawful collection, processing, storage, and transfer of personal data. This includes compliance with the DPDP Act, GDPR, CCPA, and sector-specific rules, along with drafting privacy policies, data processing agreements, and handling regulatory inquiries.

Q2 **When should a business engage a data protection lawyer in India?**

Ideally before launching any product or service that collects personal data. With the DPDP Act now in force, businesses processing Indian user data face enforceable obligations around consent, breach notification, and data principal rights. Early advisory helps avoid retrofitting compliance later.

Q3 **Which Indian law governs personal data protection and who enforces it?**

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the primary statute. The Data Protection Board of India is the designated adjudicatory body for grievances and non-compliance. The IT Act, 2000 and its rules continue to apply in certain areas until fully superseded.

Q4 **How long does a typical data protection compliance engagement take?**

A baseline privacy audit and gap analysis for a mid-size company generally takes four to eight weeks. Full implementation, including policy drafts, consent frameworks, vendor agreements, and staff training, can extend to three to five months depending on data volumes and cross-border flows.

Q5 What documents or information should a client prepare before starting?

Clients should compile existing privacy policies, data flow maps, vendor and processor agreements, consent forms, records of past breach incidents, and details of any cross-border data transfers. A current IT infrastructure overview and internal governance framework also help accelerate the initial assessment.

Q6 What common data protection mistakes do Indian businesses make?

Many businesses rely on generic consent language that fails to meet the DPDP Act's requirements for informed, specific, and freely given consent. Others neglect to maintain processing records or conduct impact assessments, which weakens their position significantly during a regulatory inquiry or breach investigation.