AILF INSIGHTS · AI AND TECHNOLOGY

Client confidentiality in the digital age: data protection for law firms

Law firms hold some of the most sensitive data in the economy. A guide to confidentiality, India's data protection law and safe use of digital tools.

A law firm's files contain trade secrets, family disputes, financial records, criminal allegations and unannounced deals. Confidentiality has always been a professional duty. It is now also a matter of data protection law and of technology.

Three layers of obligation

Professional duty. The Bar Council's rules forbid an advocate from disclosing a client's communications. The law of evidence protects professional communications from compelled disclosure.

Contract. Engagement letters and client guidelines increasingly contain detailed confidentiality and security terms.

Data protection law. The Digital Personal Data Protection Act, 2023 and the rules made under it regulate the processing of digital personal data. Law firms handle personal data of clients, opposite parties, witnesses and employees, and need to understand their obligations.

What the data protection framework expects

In broad terms, an organisation that decides why and how personal data is processed must:

- have a lawful basis, such as consent or a recognised legitimate use;
- give notice where required;
- keep data accurate and secure;
- report personal data breaches as required;
- erase data when it is no longer needed, subject to other legal requirements;
- respect the rights of individuals.

The Act contains exemptions relevant to legal work, including for processing necessary to enforce a legal right or claim. Firms should take specific advice on how the provisions apply to them.

Practical risks

- Client documents entered into public AI tools.
- Personal e-mail and messaging apps used for client work.
- Lost laptops and phones.
- Shared passwords.
- Documents sent to the wrong recipient.
- Files retained for ever, with no policy.
- Vendors with access to data and no contractual safeguards.

A baseline for every firm

- Know what data you hold and where.
- Limit access to those who need it.
- Encrypt devices and use multi-factor authentication.
- Use firm accounts, not personal ones, for client work.
- Adopt a retention and destruction policy.
- Put confidentiality and security terms in vendor contracts.
- Train everyone and repeat it.
- Have a plan for a breach, including who informs the client.

AI tools

Before using any AI service, find out whether inputs are stored, whether they are used to train the model and where the servers are. Prefer tools that keep data within the firm's control.

Why clients ask

Large clients now send security questionnaires before they engage a firm. A firm that cannot answer them will lose work, whatever its legal ability.

The principle

A client's secret remains the client's, in whatever form it is held. The medium has changed. The duty has not.

Association of Indian Law Firms · November 2026
Read online: https://indianlawfirmsassociation.com/client-confidentiality-data-protection-law-firms-india/

Keywords: data protection law firms India, DPDP Act lawyers, client confidentiality, legal privilege digital
Published by the Association of Indian Law Firms. General information only; not legal advice.