

Seclore for DPDP Compliance

[Book a Demo](#)



Persistent control of sensitive data, everywhere it travels

India's Digital Personal Data Protection (DPDP) Act has fundamentally changed how every organization handles and protects customer data. Data can no longer be "secured at the perimeter."

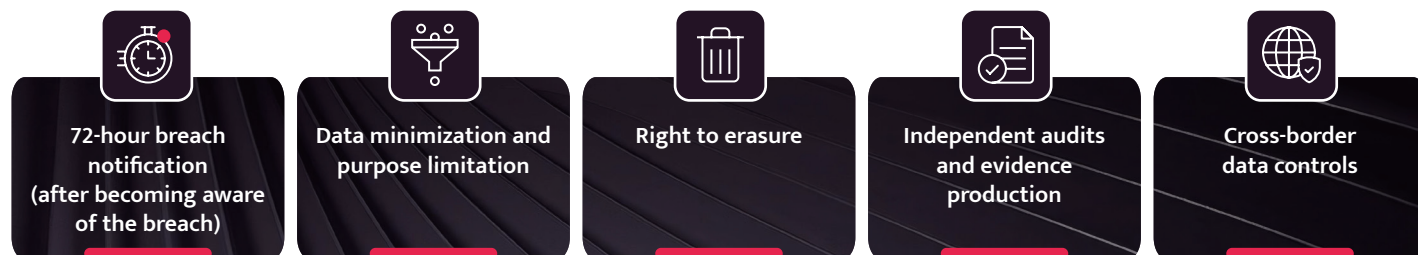
It must remain protected **everywhere it goes, at all times**, with provable controls.

With penalties of up to **₹250 crore per incident**, a single forwarded file, vendor-shared document, or delayed breach response can escalate into a board-level crisis.

Seclore enables continuous, file-level control beyond your network – the only practical way to meet DPDP obligations without slowing down the business.

The DPDP Reality: Your data leaves you every day

Every organization handling personal data is now accountable under DPDP, whether you're a bank, a healthcare provider, or a social platform, you will be treated as Data Fiduciaries under the act, with strict obligations including:



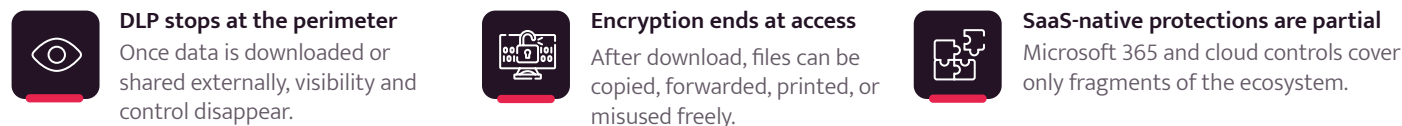
Yet sensitive data moves constantly



This is where DPDP risk compounds: You can't protect what you can't see, and you can't prove what you can't track.

Why traditional security fails DPDP

Most enterprise stacks weren't designed for DPDP. They protect the network, not the data.



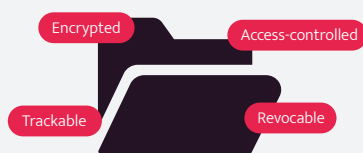
The result: • No unified data visibility • Slow, manual audits & breach workflows • No control once data leaves

DPDP's 72-hour rule = guaranteed

Seclore's approach: Protect the data itself

Once data is marked sensitive, manually or through classification, it stays:

Seclore applies data-centric security directly to the file — not just to the system around it.



Wherever it goes.

This is continuous data control. And it's the only way to enforce DPDP obligations beyond your infrastructure.

What Seclore delivers for DPDP enforcement

Seclore's platform delivers DPDP and protection through deep, file-level control and built-in auditability.



File Share Discovery + Smart Classification

Locate sensitive files across repositories and apply policy-based labels tied to purpose, data type (e.g. child data), or risk level.

Automated Protection via Enterprise Integrations

Apply protection as files move through DLP, CASB, email, identity, and ECM systems, without relying on manual triggers.



Security enforced at every touchpoint



Granular Rights Management

Define who can view, edit, copy, print, or share a file, then revoke access in real time, even post-download or post-forward.

For instance, when a collections agent downloads customer data from an internal portal, it's encrypted on the fly and logged for audit.

Evidence-Ready Audit Trails

Log every access, modification, and sharing event into a unified dashboard, built for breach response, internal audits, and DPDP assessments.



Always-on proof of control

Together, these capabilities provide **continuous proof of control**, not fragmented evidence.

What this means for DPDP compliance

With Seclore DPDP, you don't just protect data, you can show exactly how and when it was protected.

Audit-Ready Evidence, On Demand

Instant, complete proof of compliance — without manual effort.

- Immutable audit logs
- Regulator-friendly reports
- File-level lineage
- Zero missing trails

Breach Response in 72 Hours

- Instant access revocation and usage lockdown
- Real-time access logs and policy enforcement
- Even exfiltrated files remain encrypted and unreadable

Reduce penalty exposure by up to **90%**

Proven at India's leading enterprises

Organizations that manage high volumes of personal data, across finance, telecom, manufacturing, pharmaceuticals, and government, trust Seclore to enforce enterprise-wide data protection:



Auto-encrypt sensitive documents at creation



Rights management



Classify and protect email content.



Control access to PII data



Faster audits & cloud

Trusted by:

 **MARUTI SUZUKI**

 **HDFC BANK**




Reliance
Industries Limited

Safe sharing without exposure



Employees & partners collaborate freely



Every file remains traceable, revocable, and rights-bound



Accidental leaks are neutralized



Malicious misuse becomes visible and traceable

Data finally behaves as DPDP expects:
Protected by default, open only by design.



Why leaders choose Seclore

Seclore isn't another compliance checkbox. It's a control and evidence layer that works in real-world environments, where data moves fast, leaves systems, and crosses organizational boundaries.

Organizations choose Seclore because it delivers:

- Protection that travels with the file, not the network
- Rights and revocation that continue after download or forwarding
- Unified visibility from data creation to breach response
- Seamless integration into existing systems, no new habits, no extra effort

Most tools secure infrastructure.
Seclore secures your data.



Ready to prove your DPDP compliance?



DPDP isn't a policy problem, it's a data control problem.

Let's help you close the gaps, reduce risk, and show clear evidence of compliance, before the next audit or breach.