Ink.

Why every *Ink-signed* document holds up in court, the moment it's sealed.

LEG 01 · THE HANDSHAKE

Proof of *Identity*

Every signing action is gated by a per-signer HMAC v2 token cryptographically bound to ONE signer slot. The Edge Function captures the leftmost client IP, the user-agent string, and a UTC timestamp before the request body is read.

EMAIL · TOKEN · IP · UA · UTC

LEG 02 · THE CONSENT

Proof of *Intent*

Customers click through a binding clickwrap before the workspace unlocks (the six-pillar ToS shield). Signers affirm an ESIGN-equivalent consent stage before any field accepts input. Both clicks land as append-only audit rows.

CLICKWRAP · CONSENT · SHA-256

LEG 03 · THE LOCK

Proof of *Integrity*

Dual SHA-256 chain: Source SHA over the bytes you uploaded; Final SHA over the bytes the recipient receives. Server-side recomputation verifies the seal in milliseconds. Any byte change mathematically invalidates the cert.

SOURCE-SHA · FINAL-SHA · DELTA-EVIDENT

THE CRYPTOGRAPHIC TRIANGLE OF ADMISSIBILITY

PIPEDA · UECA · CANADA EVIDENCE ACT §30

THE PROMISE · THE COMMITMENT

We don't read your documents.

Not for product development. Not for sales. Not for analytics. Not for model training. Not for "QA." And not out of curiosity. Ink. personnel will not view, read, search, copy, or export the contents of your Agreement Data in the ordinary course of operating the Service.

WHEN WE DO ACCESS

You asked us to. Support ticket from you that references a specific artifact; we look at that artifact only.

We are legally compelled. Court order, search warrant, or subpoena issued by a court of competent jurisdiction in Canada. We notify you unless prohibited.

Active security investigation. Credible signal of abuse, account compromise, or breach. Minimum access necessary to contain.

The full commitment is contractually binding in the Terms §08 and the Privacy Policy §07; the long-form Q&A lives at Data management & privacy.

under two minutes.

WHAT EVERY INK-SIGNED PDF CARRIES ON ITS CERT PAGE

Every signed envelope ships its own *forensic record*.

No supplemental retrieval. No vendor support ticket. The certificate of completion appended to the last page of every Ink-signed PDF carries the dual SHA-256 hash chain, every signer's IP + user-agent + timestamp triple, the per-field signature mapping, and a chronological audit trail. Counsel reads this page once and has Sections A, B, and C in hand.

	WHAT'S ON THE CERT PAGE	WHY IT MATTERS IN COURT	STATUS
01	Source *SHA-256*	Cryptographic fingerprint of the uploaded bytes — proves what was sent BEFORE fields were placed.	LIVE
02	Final *SHA-256*	Cryptographic fingerprint of the signed + cert bytes the recipient receives — proves what was sealed.	LIVE
03	Per-signer *IP + UA*	Leftmost client IP from the proxy chain + browser/OS captured server-side at sign time. Defeats "I never saw it."	LIVE
04	UTC *timestamps* per event	Invited / opened / consented / signed — three or four timestamps per signer prove the round-trip.	LIVE
05	Per-signer *HMAC v2 token binding*	Each signing URL is cryptographically bound to one signer slot; signer-mismatch is refused at the Edge Function.	LIVE
06	Server-side *bake verification*	Redacted regions are pixel-burned server-side before any recipient delivery; integrity verified server-side.	LIVE
07	Append-only *audit_events* ledger	Postgres-backed, RLS-gated. Append-only by design — every write is an INSERT; the application has no UPDATE or DELETE path. Court-ready exhibit source.	LIVE
08	ToS *clickwrap acceptance hash*	Customer's accepted-ToS SHA-256 + UTC + IP. Material revisions force a re-accept on next login.	LIVE