



The *two-page* answer to your security and compliance review.

01 · THE THREE THINGS THAT HOLD IT UP

Built to *one* Canadian compliance shape.

PILLAR 01 · RESIDENCY

One region

Every byte of Agreement Data — documents, signers, audit events, brand assets, attachments — lives in Supabase's **AWS ca-central-1 / Montréal** project. No multi-region replication, no US warm standby, no global pod failover that quietly routes signer PII through Virginia.

CA-CENTRAL-1 · MONTRÉAL

PILLAR 02 · REGULATORY

Aligned at source

Built to PIPEDA at the federal level and Quebec Law 25 at the provincial level — both regimes assume Canadian residency. The signed-PDF audit cert calls out the alignment so the recipient sees it without having to ask.

PIPEDA · LAW 25 · UECA · CEA §30

PILLAR 03 · CONTROLS

RLS + HMAC, not a checklist

Postgres Row-Level Security gates every row by tenant membership at the database, not the app. Cross-device signing links carry an HMAC v2 token bound to a single signer and verified with a timing-safe equality check. Every signed PDF carries dual SHA-256.

RLS · HMAC V2 · AES-256 · TLS 1.2+

02 · WHAT YOU CAN HAND TO THE SECURITY TEAM

A check-by-check map of what we run.

Data resident in Canada. AWS ca-central-1, Montréal. No US routing.

AES-256 encryption at rest on the database tablespace + storage layer.

Row-Level Security in Postgres scoped to tenant_members on every read.

Dual SHA-256 fingerprints on source and final PDF bytes; both printed on the cert.

Audit-trail append-only; the cert reconstructs execution top-to-bottom.

Breach notification to you and the OPC within statutory windows.

No advertising or behavioural-tracking cookies on the marketing site or app.

PIPEDA + Quebec Law 25 alignment. Federal + provincial; same audit cert.

TLS 1.2+ in transit, no intermediate region, browser-to-Canada direct.

HMAC v2 per-signer tokens; timing-safe verification at the Edge Function.

Per-document role-based redaction with server-verified pixel-burn before delivery.

Designated Privacy Officer per Quebec Law 25 — privacy@inksign.ca.

No model training on your Agreement Data. Not ours, not third-party.

Server-side handler code reviewable on request — the scope of every Edge Function is fixed in code.

03 · WHAT YOU CAN DO

Your rights under PIPEDA and Law 25.

<p>A Access</p> <p>Receive a copy of the personal information we hold about you, in machine-readable form. We respond within 30 days.</p>	<p>B Correct</p> <p>Update inaccurate or incomplete personal information through the workspace UI or by request.</p>	<p>C Withdraw consent</p> <p>Where consent is the legal basis, withdraw it on reasonable notice. Processing stops within the same window.</p>
<p>D Delete</p> <p>Request workspace deletion. We hold a 90-day re-activation window, then purge on request or on our next scheduled pass.</p>	<p>E Portability</p> <p>Download each signed PDF (with its embedded cert) from the workspace. Workspace-level export scoped by written request.</p>	<p>F Complain</p> <p>Lodge a complaint with the OPC of Canada or the Commission d'accès à l'information du Québec.</p>

04 · WHO ELSE TOUCHES THE DATA

Our sub-processors, in full.

SUB-PROCESSOR	FUNCTION	LOCATION
Supabase Inc.	Database, authentication, storage, Edge Functions	CA-CENTRAL-1
Wildbit / Postmark	Transactional email (envelope metadata only — no PDF bytes)	USA
Stripe Payments Canada	Billing + card tokenisation (no Agreement Data)	CANADA
Netlify Inc.	Static marketing site + Next.js client bundle (no Agreement Data)	GLOBAL EDGE

05 · 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 referencing a specific artifact; we look at that artifact only.

We are legally compelled. Court order or subpoena from a Canadian court of competent jurisdiction. We notify you unless prohibited.

Active security investigation. Credible signal of abuse, compromise, or breach. Minimum necessary; documented.

06 · READ THE FULL VERSIONS

The contractually-binding documents live here.

<p>LONG-FORM</p> <h3>Privacy Policy</h3> <p>11 sections covering collection, use, location, retention, rights, our access commitment, security, and contact. PIPEDA + Quebec Law 25 aligned.</p> <p>INKSIGN.CA/PRIVACY</p>	<p>CONTRACTUAL</p> <h3>Terms of Service</h3> <p>15 sections. §08 is the contractually-binding version of "we don't read your documents." BC governing law. Lol cap = 12 months of fees.</p> <p>INKSIGN.CA/TERMS</p>
<p>FAQ</p> <h3>Data management & privacy</h3> <p>Customer-facing Q&A in DocuSign's published format, but written for our smaller-Canadian-platform reality. Best as the hand-to-IT brief.</p> <p>INKSIGN.CA/TRUST/DATA-MGMT-PRIVACY</p>	<p>COURT-BINDING</p> <h3>Legal framework</h3> <p>Why every Ink-signed PDF holds up in court. The Cryptographic Triangle of Admissibility, the audit cert structure, the three challenges and how the ledger answers them.</p> <p>INKSIGN.CA/SECURITY</p>