EASY ANNOTATION · SECURITY & PRIVACY OVERVIEW

Client Security & Privacy Packet

Architecture, technical safeguards, AI data handling, sub-processor register, and assurance status for vendor security and IT review.

PACKET VERSION	CONTROLS REVIEWED	LEGAL VERSION	PRIMARY HOSTING
v1.0	November 25, 2026	2026-11-11.1 (November 11, 2026)	AWS Canada (Central)

1. Executive Summary

Easy Annotation (Toronto, Ontario, Canada) provides PDF annotation, reference management, and AI-assisted claim substantiation tools for medical writing and scientific communications teams. Security and confidentiality controls are implemented directly across application access checks, private encrypted storage, defensive document parsing, and transparent sub-processor boundaries.

> **Core data commitment:** Customer documents are never sold, never used for advertising, and never used to train AI models. Quick Annotation runs entirely on Easy Annotation infrastructure without external AI providers.

2. Implemented Security & Privacy Controls

Encryption & Private Storage

Documents, sessions, and backups are encrypted in transit and stored in private Canadian cloud storage.

- All connections use HTTPS/TLS with HTTP Strict Transport Security (HSTS), Content-Security-Policy (restricting frame-ancestors, base-uri, object-src, and form-action), X-Content-Type-Options: nosniff, and clickjacking protection.
- Uploaded deliverables, reference PDFs, and generated outputs are stored in private AWS S3 buckets in the Canada (Central) region with server-side AES-256 encryption (SSE-S3).
- Files are never publicly browsable; downloads require an authenticated ownership or organization check, or a short-lived signed URL.
- Session cookies, two-factor secrets, and sensitive application tokens are protected with Laravel authenticated AES-256 encryption.

Tenant Isolation & Role Controls

Every workspace request is verified against the signed-in user’s ownership or organization role.

- Projects, deliverables, references, claims, highlights, exports, and billing screens enforce server-side ownership and organization scoping on every request.
- Team workspaces separate Owner, Admin, Member, and Viewer permissions; Viewers cannot alter files or reserve AI processing credits.
- Shared document invitations use 7-day HMAC-signed links bound to registered recipients, letting them create their own separate copy without modifying your original file. Sensitive auth, 2FA, invitation, and payment screens send Cache-Control: private, no-store and Referrer-Policy: no-referrer.

Authentication & Account Security

Salted password hashing, TOTP two-factor authentication, session rotation, and abuse throttling.

- Passwords are stored as salted one-way Bcrypt hashes. Password or email updates rotate remember tokens, regenerate sessions, and require email re-verification.
- Authenticator-app two-factor authentication (TOTP) with one-time recovery codes is available to all users and enforced for administrators in production.
- Rate limits protect sign-in, password reset, password confirmation, 2FA verification, online discovery, and Stripe payment confirmation; Google reCAPTCHA protects public sign-in and registration.

Zero-Training AI & Pre-Send Filtering

Your documents are never used to train AI models, and Quick Annotation never sends files to AI.

- Quick Annotation runs entirely on Easy Annotation infrastructure with no external AI calls.
- Project workspaces use DeepInfra, Inc.’s business API (we do not use OpenAI). Per DeepInfra’s published terms (checked November 11, 2026), customer text is not used to train models and prompt/response payloads are not logged or retained beyond transient serving.
- Before text is sent to AI, our privacy filter replaces project client/brand/private names, ®/™ terms, and workspace member names and emails with neutral placeholders, restoring original wording locally.
- Original uploaded files, account credentials, and billing details are never sent to AI providers.

Document Parsing & Ingestion Hardening

Uploaded documents and optional reference lookups are validated defensively before processing.

- Uploads are checked by magic-byte file signature and container validation to block spoofed formats, path traversal, symlinks, compression bombs, XML entity declarations, and external OOXML links.
- Document preview rendering runs in isolated per-job profiles after stripping external Word sub-documents, altChunks, and remote field instructions (such as INCLUDETEXT and DDE links).
- Outbound reference fetches enforce HTTPS, public-IP DNS checks (blocking private, loopback, link-local, and CGNAT ranges), redirect validation, and strict response size limits.

Backups, Deletion & Lifecycle Controls

Daily encrypted backups, self-service data export, and verifiable account deletion.

- Automated daily encrypted database backups are retained for 14 days with offsite replication and automated freshness alerts if a backup falls behind.
- Users can export their workspace data (delivered via expiring signed link) or permanently delete their account directly from account settings.
- Deleting a project or account removes primary files, cached exports, and open invitations immediately; backups and versioned objects expire within 30 days. Application logs are retained for 14 days and scrubbed for secrets before error tracking.

3. Data Boundaries & Lifecycle

Scope & Architecture Boundaries

- Not for identifiable patient records (PHI): Customers must not upload identifiable patient health information or regulated clinical records. Easy Annotation does not currently offer a HIPAA Business Associate Agreement (BAA).
- Server-managed encryption (not zero-knowledge E2EE): Files are encrypted in transit and at rest, and decrypted on our servers to parse text, render previews, generate cited copies, and run user-initiated project checks.
- Human review stays in control: Every AI suggestion is a proposal for a qualified reviewer. Medical Sign-Off records a cryptographic fingerprint of workspace edits, resolutions, and highlights so later edits invalidate sign-off before export.

Retention, Export & Deletion

- **Data residency & retention:** Primary application hosting, databases, uploaded files, and backups reside in AWS Canada (Central). Deleted primary files are removed immediately, backups age out within 30 days (14-day database backup cycle), application logs are kept for 14 days, and billing records are kept for 7 years for tax and accounting compliance.
- **Self-service export & deletion:** Export your account data or delete projects and accounts directly in Settings. Account deletion cancels active subscriptions, purges primary files and cached export archives, revokes pending invitations, and removes active workspace data unless a documented legal hold applies.
- **No ad trackers in workspaces or security pages:** Optional marketing analytics (LinkedIn Insight Tag) load only on public marketing pages after explicit opt-in consent. They never load inside signed-in workspaces, password-reset flows, legal pages, or this security page.

4. Service Providers & Sub-processors

Provider	Role	Data Handled	Region
Amazon Web Services, Inc.	Hosting, database, private S3 file storage, and encrypted backups	Account records, uploaded documents, project data, and encrypted backups	Canada (Central)
DeepInfra, Inc.	Project workspace AI claim extraction, embeddings, reranking, and evidence checks (not used in Quick Annotation)	Placeholder-filtered deliverable and reference text passages only; no original files or account PII	United States & infrastructure regions
Stripe, Inc.	Subscriptions, credit packs, invoices, payment confirmation, and fraud prevention	Billing name, email, transaction records; payment card details stay exclusively with Stripe	United States & global affiliates
Resend	Transactional email delivery (verification, password reset, invitations, receipts, export links)	Recipient email address and transactional email content	United States
Google LLC	reCAPTCHA bot protection on public sign-in/registration and support email reception	Browser/IP signals on public auth pages; messages you choose to email to support	United States & global regions

Provider	Role	Data Handled	Region
Public Literature Registries (Optional)	User-triggered Online Reference Discovery (PubMed, Europe PMC, Crossref, OpenAlex, ClinicalTrials.gov, DailyMed, FDA PMA, Health Canada)	Sanitized scientific search queries only (client, private, organization, and member names stripped; product or drug names needed for regulatory label lookups may be included); full deliverables and account PII are withheld	United States, Canada & Europe

5. Assurance Status & Honest Boundaries

Verified today: Every control described on this page is backed by implemented application code, infrastructure settings, automated PHPUnit and Python security regression tests, and blocking dependency vulnerability checks (Composer and npm audits) in CI.

Not currently claimed:

- We do not currently hold a SOC 2 Type II audit report or ISO/IEC 27001 certification.
- We do not currently offer a HIPAA BAA or a 21 CFR Part 11 / GxP computer-system validation package.
- We do not currently publish an independent third-party penetration test attestation or run automated antivirus/malware scanning on uploaded files.

As our assurance program matures, independent reports and updated attestations will be added here and in our Client Security & Privacy Packet. Security questionnaires and DPA signature requests can be sent directly to our team.

6. Incident Response & Contacts

- **Step 01 — Detect & Triage:** Automated error tracking (with token and secret scrubbing), backup freshness alerts, and security reports trigger immediate review.
- **Step 02 — Contain & Investigate:** We revoke compromised sessions, tokens, or access paths immediately and inspect scoped logs to determine root cause and affected records.
- **Step 03 — Notify Affected Customers:** Under our Data Processing Addendum and applicable privacy laws (including PIPEDA, Québec Law 25, and GDPR where applicable), we notify affected customers without undue delay with known scope, impact, and protective steps.
- **Step 04 — Remediate & Verify:** We ship targeted fixes with automated regression tests and review operational controls to prevent recurrence.

Security, Privacy & DPA Inquiries: support@easyannotation.com · **Operator:** Easy Annotation, Toronto, Ontario, Canada ·
Web Reference: /security and /legal (Terms, Privacy Policy, AI Processing Notice, Sub-processors, DPA).