Postally Security & Compliance Summary

Version 1.32 | May 1, 2026

1. Data Encryption

Postally encrypts all personally identifiable information (PII) at rest using AES-256-GCM with a dual-key architecture.

Control	Details
Algorithm	AES-256-GCM (Galois/Counter Mode) with 128-bit initialization vector and authentication tag
Key Architecture	Two independent encryption keys: personal-data-key for standard PII, phi-data-key for Protected Health Information (PHI)
Encrypted Fields	First name, last name, company, address lines (1 & 2), city, state, postal code, email, phone
Key Storage	Development: environment variables. Production: Environment variables (AWS KMS integration planned).
Key Rotation	Key ID embedded in ciphertext payload enables seamless rotation without re-encryption
Transport	All API traffic over TLS 1.2+ (HTTPS). No plaintext transmission of PII.

2. Authentication & Authorization

Control	Details
API Keys	Hashed with SHA-256 before storage. Prefix-based lookup (first 12 chars). Test and live environments separated by key prefix.
Permissions	Granular permission array per API key. Supports wildcard (*) or specific scopes (e.g., recipients.read, send.postcard).
PHI Access Levels	Four-tier hierarchy: phi_access_none, phi_access_address, phi_access_content, phi_access_full. Enforced for accounts flagged as PHI-regulated.
Email Verification	New accounts must verify email before sending mail. MX domain validation on signup rejects invalid/disposable domains. Verification link expires in 24 hours.
Session Tokens	64-character hex tokens for dashboard users. Stored with expiry and revocation tracking.
Rate Limiting	4-tier system: READ (120/60s), STANDARD (60/60s), WRITE (30/60s), EXPENSIVE (10/60s). Enforced via Redis. Returns 429 with retry-after header.
Idempotency	24-hour deduplication via Idempotency-Key header. Prevents accidental duplicate operations.

3. GDPR Compliance

Postally is designed from the ground up for GDPR compliance, supporting data processing across multiple jurisdictions.

Control	Details
Data Regions	Six supported regions: US, CA, EU, UK, AU, Other. Set per recipient.
Lawful Basis	Tracked per recipient: consent, contract, legal obligation, vital interests, public task, legitimate interests.
Retention	Configurable retention_expires_at per recipient. Automatic flagging when retention period expires.
Right to Erasure	POST /v1/gdpr/erasure permanently destroys all PII. Cascades to mailpiece snapshots, S3 PDFs, and QR analytics.
Right to Access	GET /v1/gdpr/access returns all stored data including mail history, group memberships, and sub-processor list.
Data Portability	GET /v1/gdpr/export provides machine-readable JSON download per Article 20.
Sub-Processors	Documented: print house, Smarty (address verification), Stripe (payments), AWS (storage, email).
DPA Support	Immutable audit log tracks every personal data access for Data Processing Agreement compliance.

4. PHI-Aware Data Handling

Important: Postally is NOT HIPAA-certified and does not act as a HIPAA-covered entity or business associate. Postally does not currently offer Business Associate Agreements (BAAs). The controls below describe PHI-aware data-handling features available to accounts that need to handle health information internally. Customers must independently determine whether the Platform meets their compliance obligations. Do not transmit Protected Health Information through the Platform without first contacting support@postally.ca to discuss your use case.

Control	Details
Dual Encryption	PHI encrypted with a separate phi-data-key. Standard PII uses personal-data-key. Keys never shared.
PHI Access Levels	Four-tier RBAC (none / address / content / full). API keys restricted to minimum necessary PHI access.
BAA Status Tracking	Internal hipaa_baa_signed_at / hipaa_baa_document_url fields exist on the account schema for accounts that have signed BAAs with their own downstream parties; Postally itself is not a party to those BAAs.
Disclosure Accounting Endpoint	GET /v1/hipaa/disclosure-accounting returns every PHI disclosure (to print house, Stripe, address verification): recipient, fields, timestamp, purpose.
Print House Routing	Pieces flagged contains_phi=true are blocked from print houses without an internal BAA flag, and disclosure events are logged when transmitted.
Minimum Necessary	Audit log records justification for each PHI access. Only required fields are decrypted.

5. Audit & Operational Controls

These controls align with industry security frameworks (e.g., SOC 2 trust principles), but Postally has not undergone a SOC 2 audit. The controls themselves are real and operational; the certification is not.

Control	Details
Immutable Audit Log	PostgreSQL triggers prevent UPDATE and DELETE on audit_log table. Every personal data access logged.
Audit Archival	Audit logs shipped to S3 with Object Lock (WORM) for tamper-proof long-term storage. Requires S3 bucket configuration with Object Lock enabled. The application validates and falls back gracefully if not configured.
RBAC	Role-based access control via API key permissions and PHI access levels.
Rate Limiting	Prevents abuse and DoS. 4-tier system: READ (120/60s), STANDARD (60/60s), WRITE (30/60s), EXPENSIVE (10/60s).
Monitoring	Pino structured logging with JSON output in production. Server request logging and error tracking.
Change Management	Git version control with branch protection on main.

6. PCI DSS

Control	Details
Compliance Level	SAQ A (Self-Assessment Questionnaire A) via Stripe.
Card Data	No credit card numbers, CVVs, or cardholder data ever touch Postally servers.
Payment Processing	All payments handled by Stripe Checkout sessions. Customers enter card details on Stripe-hosted pages.
Stripe Integration	Webhook signature verification (HMAC-SHA256) for all payment events.

7. Additional Security Measures

Control	Details
Soft Deletes	Resources are soft-deleted (deleted_at timestamp), never hard-deleted, preserving audit trail.
Request Correlation	X-Request-Id header on every request for complete request tracing.
Graceful Degradation	External services (S3, SES, Smarty, Stripe) fail gracefully without exposing errors.
Retry with Backoff	External API calls use exponential backoff with jitter to prevent thundering herd.
Input Validation	All inputs validated with Zod schemas. Invalid input rejected before processing.
Content Moderation	All uploaded images and design captures are automatically scanned by AWS Rekognition for NSFW/offensive content. Content detected at 50% or higher confidence (nudity, violence, hate symbols, drugs) is blocked immediately and cannot be printed.
S3 Object Lock	Audit logs and compliance documents stored with WORM (Write Once Read Many) protection. Requires S3 bucket configuration with Object Lock enabled. The application validates and falls back gracefully if not configured.

8. Canada Post Personalized Mail Eligibility

Postally offers two mail classes for postcards and letters: Lettermail (first_class) and Personalized Mail (standard). Canada Post restricts Personalized Mail by both CONTENT TYPE and MINIMUM QUANTITY. Customers are responsible for correct classification; misclassified mail may be refused, surcharged, or redirected by Canada Post, and Postally may pass those charges through to the customer's account.

8.1 Content Restrictions

Personalized Mail is only eligible for ADDRESSED MARKETING / PROMOTIONAL content. Transactional, personal, and general correspondence must use Lettermail.

Category	Examples	Eligible for Personalized Mail?
Promotional / Marketing	Sale announcements, event invites, catalogs, newsletters, loyalty promotions, product launches	YES (if quantity ≥ 125 pieces)
Transactional	Invoices, statements, payment reminders, account notices, shipment confirmations, legal notices	NO — Lettermail only
General correspondence	Personal letters, appointment reminders, thank-you notes, welcome letters, survey requests	NO — Lettermail only

8.2 Quantity Minimum

Canada Post's published minimum for Personalized Mail is 100 pieces. Postally enforces a 125-piece minimum internally — a 25-piece safety buffer above Canada Post's floor to absorb SmartyStreets address-verification dropouts on poorly-hygiened lists. Mailings with fewer than 125 pieces must use Lettermail (which has no piece minimum and works for any content type).

8.3 Phantom Charge Risk

Canada Post applies a FLAT 100-piece minimum charge to Personalized Mail regardless of actual quantity. A mailing of 10 Personalized Mail pieces is billed at 100 × per-piece rate, not 10

× per-piece rate. The 125-piece Postally floor eliminates this phantom charge risk entirely — customers never see a Personalized Mail price for a mailing that would incur the phantom fee.

8.4 Customer Attestation

When selecting Personalized Mail ('standard' mail_class) for eligible mailings, customers must confirm the following attestation before campaign creation or order checkout:

"I confirm this mailing is addressed marketing/promotional content and complies with Canada Post's Personalized Mail eligibility requirements. I understand that misclassified mail may result in additional Canada Post charges, surcharges, or refusal, and that Postally may pass those charges through to my account."

The attestation is captured at campaign create time (campaigns.attestation_accepted_at timestamp) and order create time (metadata.attestation_accepted_at). A separate audit log action (campaign.attestation_accepted) records every attestation for compliance queries.

8.5 Enforcement

Policy enforcement runs at every entry point that creates mailpieces:

Entry point	Enforcement
POST /v1/campaigns/create	Rejects mail_class='standard' for campaigns below the 125-piece floor or with non-promotional content_category. Attestation required.
PATCH /v1/campaigns/:id	Re-validates on every draft-phase update. Campaigns in post-draft states must revise first.
POST /v1/orders/create	Same policy as campaigns. Validated at cost preview, before Stripe checkout.
POST /v1/postcards/create, /v1/letters/create	Single sends are 1 piece — mail_class='standard' is always rejected.
POST /v1/postcards/batch, /v1/letters/batch	Batch-level policy: entire batch must meet the floor if any item uses 'standard'.
POST /v1/pricing/quote	Returns policy verdict alongside the estimate so dashboards can render comparison cards and warnings.
Klaviyo webhook (/v1/triggers/klaviyo)	Always defaults to Lettermail — Klaviyo events are 1 piece by definition.

Entry point	Enforcement
Stripe order fulfillment (webhook)	Inherits the order's validated mail_class and passes the true piece count so service-level checks don't re-reject.

8.6 Misclassification Liability

If a customer misclassifies a mailing (for example, selects 'promotional' for content that is actually transactional), and Canada Post flags the mailing, the following consequences apply:

- Canada Post may refuse delivery and return the mailing to Postally.
- Canada Post may apply a surcharge equal to the difference between the billed rate and the correct Lettermail rate.
- Postally may pass through any Canada Post surcharges to the customer's account as a line-item charge.
- Repeat misclassification may result in account suspension or termination.

Customers who are unsure about their content category should contact support@postally.ca before submitting a mailing.