

In plain language

Working copies of your request and records are kept 14 days after delivery, then deleted.

Package access follows the order window you bought.

Backups follow a separate, shorter cycle.

Payment records are kept for accounting.

The tables below are the periods that apply.

Data Retention and Deletion Policy

Version 2026-09-25.2 · Effective 2026-09-25.2

Scope: Lifecycle rules for Fit Check files, source records, packages, billing, support, logs, and deletion requests.

Policy contact: privacy@attestlayer.com

Related:

Privacy Notice

· Direct-Client Data Processing Addendum

· Subprocessors

Email verification and Fit Check records

- Email-verification challenge rows are deleted after seven days.
- Unused Fit Check results and sign-in sessions expire and are deleted about 30 days later if no order was placed. A Fit Check result linked to a paid order is kept with that

order's records (see Billing records).

Request-fit files

We keep a working copy of your request and records for 14 days after delivery so reruns work without re-uploading, then delete it. The fit result and limited operational metadata may remain with security, support, or order records as described below.

Source uploads

We keep a working copy of your request and records for 14 days after delivery so reruns work without re-uploading, then delete it. Files explicitly marked as downloadable evidence may be copied into the generated private ZIP.

Generated output

Your generated packages stay available in the Client Console until the later of the end of your order window or 30 days after your most recent finalized package. After access ends, the package files enter deletion; an administrator can recover them for 7 days, then they're gone.

Private package storage enters asynchronous lifecycle deletion after access ends and a seven-day provider soft-delete recovery window, with Console access disabled during that recovery period. Order, package-identifier, billing, and integrity metadata may be retained separately for the periods below or where law requires it.

Working copies of client-request and source files are kept for 14 days after delivery by default, and are then deleted. Same-request reruns stay available for the whole purchased order window: 90 days for a new single Full review and 12 months for Three-Pack and Five-Pack. Essentials and Integrity Check include no reruns. After that 14-day hold ends, a rerun needs the authorized source records submitted again.

Human-support records

A human-support ticket may include the requester's business contact details, message, safe route and order references, selected decision concern, assigned queue, response state, and provider delivery events. The selected concern is only a classification and versioned response aid for the human operator; it does not choose the assigned queue and is not used for routing the request or changing Fit Check, price, eligibility, or evidence classification.

Tickets marked resolved or closed, their delivery records, and their selected concern become eligible for deletion one year after recorded resolution and to be deleted no later than two years after creation. Open or reopened tickets use the two-year maximum rather than being treated as resolved. A legal hold can pause deletion until the hold ends. These periods are separate from the seven-year paid-order and accounting period below.

Measurement and optional public analytics

Fit measurement rows for `fit_started`, `fit_passed`, and `fit_failed_reason` are retained for no more than 30 days. These measurement rows are distinct from separately governed paid Fit, order, invoice, and entitlement authority metadata. Other first-party usage measurements (counts of page views and product steps, never file contents) are kept for no more than 13 months.

Optional analytics uses a consented same-origin first-party relay only on these approved non-sensitive public routes: `/`, `/buyer-review-pack`, `/choose-the-right-workflow`, `/faq`, `/how-it-works`, and `/what-you-receive`. The browser loads no PostHog browser SDK or other third-party analytics code. The browser sends no client-request, source-record, evidence, evidence-binder index, generated statement, manifest, receipt, or package content through the analytics path to the relay or analytics provider.

A consent grant is bound to the current Cookie Notice and legal-policy version. A stale grant causes the site to re-prompt before optional analytics can resume. Revocation removes the signed server consent authority and stops future collection, but does not retroactively delete or alter events lawfully collected before withdrawal. Optional analytics consists only of low-cardinality events tied to an anonymous consent session. Under the current provider plan, those events may be retained for up to 12 months.

Billing records

Paid Fit Check and order metadata, purchase intents, Stripe event references, entitlements, email delivery records, resolved operational alerts, provider delivery metadata, and payment, invoice, refund, tax, and accounting records are ordinarily retained for seven years. This period supports billing, accounting, fraud prevention, service integrity, customer support, and dispute handling. A record may be retained longer where law requires it or a preserved legal hold applies. We also keep the client organization name, request type and finalization date for 2 years to send one renewal reminder; you can turn this off in the Console.

Transactional email delivery

A definitive pre-acceptance email rejection is safely retryable. An ambiguous transport result is quarantined for manual reconciliation and is never blindly auto-resent. SendGrid processed or accepted means the provider accepted the message for handling; it does not prove inbox delivery. Only a provider delivered event marks the message delivered. Provider message identifiers, attempt state, delivery outcome, bounce, and complaint metadata follow the paid-order retention period above.

Security logs

Security and abuse-prevention logs are retained for up to 90 days unless an investigation, dispute, fraud-prevention need, documented legal hold, or law requires longer.

Registry commitments

Where an issued package includes a public Registry commitment, its cryptographic hashes, signature material, and status may remain indefinitely so third parties can continue to verify integrity. Registry commitments do not contain submitted source files or recoverable source content.

Deletion requests

For personal-information requests, email privacy@attestlayer.com. AttestLayer may retain limited information where required for law, accounting, security, fraud prevention, or dispute resolution.

 **Talk to a human**