

Buyer Review Pack security and data handling

Version 2026-09-30.3 · Effective 2026-09-30.3

Scope: Current and unavailable safeguards, request-byte handling, package storage, access, signing, verification, and assurance boundaries.

Policy contact: security@attestlayer.com

Related:

Privacy Notice

- Direct-Client Data Processing Addendum
- Subprocessors
- Data Retention and Deletion Policy
- Vulnerability Disclosure Policy

A record-only service designed to minimize access, isolate customer packages, and make issued output verifiable against separately published key material.

At a glance

Swipe or use arrow keys to view all columns

Control	Status	Verify it
Administrator accounts protected by hardware security keys	In place	Security page

Control	Status	Verify it
Operator actions require a passkey and an allowlisted network	In place	Security page
Customer sign-in: single-use link, 15-minute expiry; sessions 30 min idle / 12 h	In place	Security page
Order database encrypted with a customer-managed key (Cloud KMS)	In place	Security page
Daily backups with point-in-time recovery; 30 retained; last restore test not yet recorded	In place	Security page
Security logs kept 90 days; access to customer files logged	In place	Security page
Public site loads no third-party scripts; strict CSP, HSTS preload	In place	View headers
SPF, DKIM, DMARC on attestlayer.com	In place	DNS
72-hour breach notification	Contractual	DPA §9
Sub-processors published, change notice before processing	In place	Subprocessors
Vulnerability disclosure policy and security.txt	In place	security.txt
No security incident affecting customer data as of 2026-10-01	Statement	Security page
Package signing keys in Secret Manager; public keys published with validity dates	In place	Registry

Direct-client and Console scope

The standard Buyer Review Pack does not require access to customer production systems, installed endpoint software, production credentials, or source-code repositories. Customers submit only the records authorized for one eligible client review through the secure Console.

Accepted inputs and authorization

Client Console keeps the client request, any required completed response, and supporting source records in separate upload slots. Only the purchasing organization's verified, order-authorized session may access its order and package workflow. Customers must submit only records they are permitted to use for that client review.

Supported formats, size limits, hidden-content checks, archive limits, malware checks, and prohibited-content rules are enforced before generation. Do not upload credentials, secrets, private keys, payment-card data, health data, source code, production access, or unauthorized records.

Storage, encryption, and tenant boundary

The direct-client workflow uses Google Cloud resources in Montréal for application processing, private object storage, and the order database. HTTPS protects data in transit. The order database is encrypted at rest with a customer-managed key in Cloud KMS. Secrets and object storage use Google-managed encryption. Public access prevention, authenticated package access, tenant-scoped order checks, least-privilege service identities, and separately managed secrets constrain access.

Automated processing and review

No AI model reads your records. Parsing, classification, drafting and checking of your questionnaire and records run as versioned, deterministic rules inside AttestLayer's own Google Cloud project in Montréal. The service that processes your files has no access to any AI model service.

Verified on 2026-09-30 by a dependency scan of every service that handles customer files: no model SDK is imported and no customer file is sent to a model host. The attestation table is available on request.

Generation is automated and may classify requirements, select source passages, draft source-linked responses, and identify gaps. It does not establish that a source record is true. The customer reviews every proposed answer and evidence decision before creating the final client-forwardable package. See the [Automated Processing Notice](#).

Retention and deletion

We keep a working copy of your request and records for 14 days after delivery so reruns work without re-uploading, then delete it. Generated package access follows the order window. Package objects, email challenges, session/fit records, transaction metadata, backups, lawful holds, and deletion recovery have different lifecycle rules. The exact categories and periods are published in the [Data Retention and Deletion Policy](#).

Payments, email, and subprocessors

Stripe handles payment-card details. SendGrid handles transactional email. Google Cloud hosts the application and protected data path. No public analytics provider receives customer source records from this workflow. Current provider purposes and locations are listed on the [Subprocessors](#) page.

How access and keys are protected

Operator actions on the Control Desk require a passkey (phishing-resistant, bound to a registered credential) and are accepted only from an allowlisted network.

Customers sign in with a single-use email link that expires after 15 minutes. Sessions end after 30 minutes of inactivity or 12 hours at most. We store only hashes of the link and the session secret.

Package signing keys are held in Secret Manager; only the public keys are published, in the Registry, each with its key ID and validity dates.

The order database is encrypted at rest with a customer-managed key in Cloud KMS. Secrets and object storage use Google-managed encryption.

La base de données des commandes est chiffrée au repos avec une clé gérée par le client dans Cloud KMS. Les secrets et le stockage d'objets utilisent le chiffrement géré par Google.

The order database is backed up daily (03:00 UTC) with point-in-time recovery; transaction logs are kept 7 days and 30 backups are retained.

Security and abuse-prevention logs are kept for up to 90 days. Access to customer files is logged.

The Google Cloud and Google Workspace administrator accounts are protected by hardware security keys.

Les comptes administrateur Google Cloud et Google Workspace sont protégés par des clés de sécurité matérielles.

No security incident affecting customer data has occurred as of 2026-10-01.

Aucun incident de sécurité touchant des données clients n'est survenu en date du 2026-10-01.

Security and package-integrity practices

- HTTPS transport. The order database is encrypted at rest with a customer-managed key in Cloud KMS. Secrets and object storage use Google-managed encryption.
- Private object storage, public-access prevention, authenticated package access, and tenant-scoped authorization.
- Least-privilege service identities, separately managed secrets, restricted administrative access, and separation between public, checkout, Console, verification, and processing roles.

- Processing is automated. The founder may open delivered packages for quality control, under the same confidentiality obligations as the Service. No one else at AttestLayer has access to your records or packages.
- Business-email access verification, signed payment-webhook verification, replay and duplicate-event protection, and order-capacity reconciliation.
- Canonical manifests, SHA-256 file hashes, signed receipts, issuer-key separation, hosted and offline verification, and intentional-tamper rejection.
- Security logging, incident handling, controlled suspension, rollback, and recovery procedures.

Incident and vulnerability contact

Report a suspected product-security incident or data-handling concern to security@attestlayer.com. Do not include secrets or confidential source records in ordinary email. Security researchers should follow the [Vulnerability Disclosure Policy](#).

Current assurance boundary

AttestLayer does not currently have:

- SOC 2 (Type I or II), ISO/IEC 27001 or CSA STAR;
- an independent penetration test or external assurance opinion;
- cyber or technology errors-and-omissions insurance.

AttestLayer does not currently hold cyber or professional liability insurance. The liability limit in the Terms of Service applies.

No AI model reads your records. Extraction, matching, and checks run in this service.

AttestLayer does not currently claim or display completion badges for SOC 2, ISO/IEC 27001, an independent penetration test, or insurance.

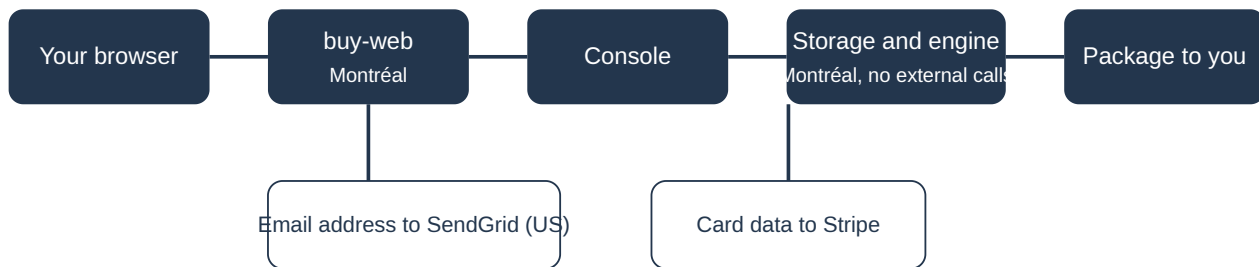
A PACKAGE INTEGRITY VERIFIED result confirms the package checks identified by the verifier. Buyers can repeat that check with the hosted verifier. It does not certify compliance, establish that submitted records are true, or guarantee client acceptance.

Public site

The public site loads no third-party scripts.

Where records are processed

Records are processed in Canada. Customer questionnaires and records are stored and processed in Montréal (northamerica-northeast1). Business email addresses go to SendGrid. Card and invoice data go to Stripe. See the Data Processing Addendum for the 72-hour breach notice.



Customer questionnaires and records are stored and processed in Montréal. Business email addresses go to SendGrid. Card and invoice data go to Stripe.

DPA and further questions

The direct-client Data Processing Addendum and the policies linked above describe the standard public terms. Email security@attestlayer.com to request further security material; an NDA is available. Completed answers about AttestLayer are on the [security questionnaire](#).

 **Talk to a human**