

In plain language

This addendum applies when AttestLayer processes personal data for your order.

You decide which records are authorized for that order.

We notify you within 72 hours after confirming a personal-data breach.

Subprocessors are listed on the subprocessors page.

A countersigned PDF is available on request.

Standard direct-client terms

Data Processing Addendum

Version 2026-09-30.1 · Effective 2026-09-30.1

Scope: Customer personal data processed for the direct-client Buyer Review Pack workflow.

Policy contact: privacy@attestlayer.com

Related:

Terms of Service

· Privacy Notice

· Subprocessors

· Data Retention and Deletion Policy

· Security and Data Handling

Version 2026-09-30.1 · English controlling copy · Rabie-Abdollah Macbahi, doing business as Services AttestLayer ('AttestLayer')

This Data Processing Addendum (DPA) forms part of the AttestLayer Terms of Service (Terms) only when an eligible customer validly accepts the exact version identified in its order record. It governs Customer Personal Data processed by Services AttestLayer, operating as AttestLayer (AttestLayer), on the customer's behalf for that order. Capitalized terms not defined here have the meaning given in the Terms.

1. Definitions and roles

Customer Personal Data means personal data or personal information that AttestLayer processes on the customer's behalf through the enabled direct-client service. **Applicable Data Protection Law** means privacy or data-protection law that applies to that processing. **Subprocessor** means a third party engaged by AttestLayer to process Customer Personal Data on AttestLayer's behalf.

The customer is the controller or business and AttestLayer is the processor or service provider for Customer Personal Data, except where Applicable Data Protection Law assigns a different role for a specific activity. Each party remains responsible for its independent legal obligations. AttestLayer acts as an independent controller for its own account, payment, fraud-prevention, security, tax, and legal-compliance records where the law so provides.

2. Scope, subject matter, and duration

This DPA covers the eligible Integrity Check, Buyer Review Essentials, Full Buyer Review Pack, Three-Pack, and Five-Pack expressly enabled in the order. Processing is limited to Fit-authorized intake, validation, package generation, customer review and finalization, private delivery, support, integrity verification, security, and the other purposes in Annex A. It begins when a valid order is activated and ends after the Service and applicable retention periods end, subject to legal retention duties and protected backup cycles.

3. Documented instructions

AttestLayer will process Customer Personal Data only on documented instructions from the customer as expressed by the Terms, this DPA, the accepted order, authorized use of the Service, and written support instructions. AttestLayer will promptly inform the customer if it reasonably believes an instruction violates Applicable Data Protection Law, and may suspend that instruction while the parties resolve it. If law requires processing outside the customer's instructions, AttestLayer will inform the customer before processing unless the law prohibits notice on important public-interest grounds.

AttestLayer will not sell or share Customer Personal Data for cross-context behavioural advertising, retain, use, or disclose it outside the direct business purposes described in this DPA, or combine it with personal information received from another person except as permitted by Applicable Data Protection Law to provide or secure the Service.

4. Confidentiality and personnel

AttestLayer will limit access to personnel who need it to provide, secure, or support the Service. Authorized personnel will be bound by confidentiality obligations or an appropriate statutory duty, receive role-appropriate security and privacy instructions, and process Customer Personal Data only as authorized.

5. Security measures

Taking account of the nature, scope, context, and purposes of processing and the risk to individuals, AttestLayer will maintain the technical and organizational measures in Annex B. The measures are contractual requirements for an activated order, not a certification or a claim that an not available control, audit, or third-party assessment has been completed. AttestLayer may update a measure without materially reducing the overall protection of Customer Personal Data.

6. Subprocessors

The customer gives general written authorization for the subprocessors on the current [Subprocessors page](#). AttestLayer will impose written data-protection duties that provide protection appropriate to the processing and will remain responsible for a

subprocessor's performance of those duties as required by Applicable Data Protection Law.

AttestLayer will publish an intended addition or replacement before that subprocessor begins processing Customer Personal Data when applicable law requires an objection opportunity. The customer may send a reasonable, law-based objection to privacy@attestlayer.com. The parties will work in good faith on a commercially reasonable resolution. If none is available, either party may terminate the affected unperformed processing, with any refund governed by the accepted Refunds and Billing Policy and mandatory law.

7. Requests from individuals

Taking account of the nature of the processing, AttestLayer will provide reasonable technical and organizational assistance for the customer to respond to requests to access, correct, delete, restrict, port, or object to processing of Customer Personal Data. If AttestLayer receives a request relating to Customer Personal Data, it will direct the requester to the customer when permitted and will not respond on the customer's behalf unless instructed or legally required.

8. Compliance assistance

Taking account of the processing and information available to AttestLayer, AttestLayer will provide reasonable assistance with security obligations, personal-data-breach assessment and notice, data-protection impact assessments, and prior consultation with a regulator where Applicable Data Protection Law requires that assistance. Assistance beyond standard documentation and support may require a separately agreed scope and reasonable fees, unless the need was caused by AttestLayer's breach of this DPA.

9. Personal data incidents

AttestLayer will notify the affected customer without undue delay, and in any case within 72 hours, after confirming a breach of security that results in accidental or

unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. Notice will include available information reasonably needed for the customer's obligations, and may be provided in phases as facts become available. Notice is not an admission of fault or liability.

10. Return, deletion, and retention

At the customer's choice and subject to Service functionality, AttestLayer will return or make available Customer Personal Data and delete remaining copies after the applicable Service and retention period. The Data Retention and Deletion Policy states the standard lifecycle. Copies that law requires AttestLayer to keep, and protected backups awaiting their normal deletion cycle, will remain isolated from ordinary use and protected under this DPA.

11. Information and audits

AttestLayer will make information reasonably necessary to demonstrate compliance with this DPA available through its published security, privacy, subprocessor, retention, and verification materials and reasonable written responses. If those materials are insufficient for a requirement that applies to the processing, the customer may request one audit per year by an independent qualified auditor, on reasonable notice, during business hours, under confidentiality, and without access to another customer's data or material disruption. The customer bears its audit costs unless the audit identifies AttestLayer's material breach. No on-site audit or custom security assessment is included in the standard self-serve price, but this sentence does not limit a non-waivable statutory right.

AttestLayer will promptly tell the customer if, in its opinion, an instruction infringes Applicable Data Protection Law. Nothing in this section represents a completed SOC, ISO, penetration test, certification, or independent assurance report.

12. International and interprovincial transfers

Processing locations and provider roles are disclosed on the Subprocessors page. Each party will satisfy the transfer requirements that apply to it. The customer is responsible for any required privacy impact assessment before directing a transfer outside Quebec or another restricted jurisdiction. AttestLayer will provide reasonable information about contractual and technical safeguards for that assessment. If a transfer requires standard contractual clauses, a United Kingdom addendum, or another statutory mechanism not included in the standard order, the customer must not submit the affected data until the required mechanism is validly completed.

13. Legally compelled disclosure

AttestLayer will assess a binding government or legal demand for Customer Personal Data, disclose only what it is legally required to disclose, and notify the customer before disclosure where legally permitted. AttestLayer will use reasonable measures to challenge an overbroad demand when there are lawful grounds and a reasonable prospect of limiting it.

14. Customer responsibilities and prohibited data

The customer warrants that it has authority and a lawful basis to provide the data and issue its instructions, gives required notices, responds to individuals, and limits submissions to what is necessary. The standard service does not authorize credentials, secrets, private keys, payment-card data, government identification numbers, health or medical data, highly sensitive personal data, regulated records, source code, or another person's data that the customer is not authorized to disclose. The customer must use the secure Console, not email or support forms, for authorized Service inputs.

15. California service-provider terms

To the extent the California Consumer Privacy Act applies and AttestLayer is a service provider or contractor, the customer discloses Customer Personal Data only for the limited and specified business purposes in Annex A. AttestLayer will comply with applicable service-provider restrictions, provide the same level of privacy protection

required by applicable law, notify the customer if it can no longer meet those obligations, and allow the customer to take reasonable steps to stop and remediate unauthorized use.

16. Term, conflict, and liability

This DPA continues while AttestLayer processes Customer Personal Data for the order. If it conflicts with the Terms on protection or processing of Customer Personal Data, this DPA controls to that extent. A separately signed agreement controls only where it expressly identifies the affected term and order. The limitations of liability in the Terms apply to this DPA to the maximum extent permitted by law; this DPA does not reduce a right or obligation that cannot lawfully be limited.

17. Acceptance and version binding

Downloading this document does not create an order or authorize processing. For an eligible standard order, acceptance is recorded with the accepting organization, verified business email, acceptance time, DPA version and source hash, artifact revision and PDF hash, policy- manifest hash, catalog version and hash, payment reference, and tamper-evident acceptance- record digest. The DPA binds only when it is incorporated into an eligible accepted order. Contact privacy@attestlayer.com for privacy questions or security@attestlayer.com for security questions.

Annex A - Processing details

Subject matter: the direct-client record-only review-package workflow for the exact product in the accepted order.

Duration: the activated order and the documented retention and deletion lifecycle.

Nature and purposes: receive authorized records; validate format, scope, malware, hidden content, and lineage; preserve or generate the product-specific output; support customer review and correction; finalize, sign, privately deliver, and verify the package; prevent abuse; provide support; and maintain security, billing, tax, and legal records.

Data subjects: customer personnel, business clients or prospective clients, business contacts, and individuals whose limited business information appears in authorized records.

Personal-data categories: names, business contact details, job titles, employer and role information, order and access records, client-request text, authorized source-record content, customer-completed response text, support communications, and security or audit metadata.

Special-category and regulated data: not authorized under the standard service.

Customer rights and obligations: determine purposes and lawful basis, give lawful instructions and notices, ensure accuracy and minimization, control authorized users, respond to individuals, and download outputs before expiry.

Annex B - Technical and organizational measures

Encrypted network transport and managed encryption at rest for supported storage and databases.

Private object storage, public-access prevention, authenticated package access, bounded signed access, and tenant-scoped authorization.

Least-privilege service identities, separately managed secrets, restricted administrative access, and separation of public, checkout, Console, verification, and internal processing roles.

Business-email access verification, signed webhook verification, replay and deduplication controls, exactly-once entitlement checks, and order-capacity controls. Input size, type, schema, hidden-content, malware, and prohibited-content validation that fails closed before processing.

Deterministic package manifests, file hashes, signed receipts, issuer-key separation, hosted and offline verification, and intentional-tamper rejection.

Security and access logging, incident handling, reconciliation, rollback, and controlled service-suspension procedures.

Managed backups and point-in-time recovery where applicable, documented restoration procedures, retention schedules, and deletion controls.

Availability, workload isolation, and concurrency controls appropriate to the purchased service capacity.

Vendor due diligence and written subprocessor obligations proportionate to the services they provide.

Document control

Canonical page: <https://buy.attestlayer.com/dpa>

Standard PDF: <https://buy.attestlayer.com/api/legal/dpa/pdf>

Machine-readable metadata: <https://buy.attestlayer.com/api/legal/dpa/metadata>

Services AttestLayer is the registered business name of Rabie-Abdollah Macbahi, a sole proprietor registered in Québec (NEQ 2282022963), 360 Saint-Jacques Street, Suite G101, Montréal, QC H2Y 1P5.

Head office: 360 Saint-Jacques Street, Suite G101, Montreal, Quebec H2Y 1P5, Canada

Version and effective date: 2026-09-30.1

A countersigned PDF of this DPA is available on request: security@attestlayer.com.

 **Talk to a human**