SafeGora Named Consultant Agreement

OllieLabs LLC, operating as SafeGora

Version 2026-10-23.4 | Effective Date October 23, 2026

Documents in this Agreement

1 Home Agreement and full Named Seat Rider
2 Terms of Service
3 Privacy Notice
4 Refund and Cancellation Policy
5 Data Processing Addendum and Annexes A–E

SafeGora Named Consultant Home Agreement

Document identifier sg-consultant-home

Version 2026-10-23.4

Effective Date October 23, 2026

1 Your agreement

This Home Agreement is between OllieLabs LLC, operating as SafeGora, and the consulting firm identified in the accepted Order. The person accepting for the firm must be authorized to bind it. Accepting for the firm does not create a personal payment guarantee.

This version is for New Firms. “New Firm” means a consulting firm that first accepts this version and begins its trial on or after the Effective Date shown on this document. A later paid election and properly accepted quantity changes for that subscription use the same accepted agreement. Existing customers, existing trials, historical partner plans, employer subscriptions and earlier commitments keep their applicable terms. Servicing an existing contract does not adopt this version. Publication, a renewal, payment or a saved card does not replace an earlier acceptance record.

The Agreement includes this Home Agreement, the Named Seat Rider, the accepted Order, and the SafeGora Named Consultant Terms of Service, Data Processing Addendum, Privacy Notice, and Refund and Cancellation Policy, each identified by version before acceptance. Their express commitments, including those in the accepted Privacy Notice, are contractual. The common version is 2026-10-23.4. The Terms define the capitalized expressions used here.

The documents must be available to read and retain before the firm accepts. The recorded Order identifies the firm, its authorized representative, the accepted documents and the commercial terms. Agreement acceptance and authorization for paid subscription charges are separate decisions. Acknowledging the Privacy Notice does not authorize unrelated uses of personal data.

2 Your practice and client work

Firm OS provides the firm's practice workspace and named-user access for its own business and authorized consulting work for employer clients. It is a software subscription. It does not appoint SafeGora as the firm's legal adviser or safety professional, or make a consultant SafeGora's employee or agent.

Each employer controls access to its records. The employer's actual permission, the user's assigned role and the available service function must permit the work. Buying a consultant license does not itself grant client access or authority to certify, submit, post or delete an employer record. The firm remains responsible for its professional engagement; the employer retains its own review, certification, filing, posting and retention responsibilities.

An employer may narrow or revoke its permission. Corresponding consultant access then narrows or ends, even if the firm still has paid licenses. This does not transfer ownership of the employer's records or erase required audit history. A later engagement needs valid permission again.

Employer subscriptions, the firm's own client fees and any commission arrangement are separate. This subscription does not create a commission entitlement, guarantee client introductions, authorize an employer's payment, or offset a commission against the firm's fees.

3 Personal data and service commitments

The DPA and its standard processing schedule apply to the accepted Customer and Order, together with the employer permissions actually granted. The firm must provide accurate account information and upload only information it is authorized to use for the agreed work. Additional processing outside that agreed scope needs the required agreement and safeguards before it begins.

The Terms and DPA set the parties' confidentiality, security, information-use and data-return duties. This Home Agreement makes no separate uptime, response-time, restoration or service-credit promise. Liability limits, indemnities, exclusions, dispute resolution and governing law are set out in the Terms; this Home Agreement creates no additional liability cap or unlimited indemnity.

4 Ending service and preserving records

The Rider and Refund and Cancellation Policy explain ordinary cancellation. The Terms also provide termination rights and agreed refunds, including the applicable remedies for SafeGora's uncured material breach, early termination without Customer Cause, as defined in the Terms, and an unresolved covered intellectual-property claim. The DPA provides its subprocessor-objection remedy. These express refunds are entitlements when their conditions are met and need no additional discretionary approval.

The firm has the data-return opportunity provided in the Terms and DPA, including at least thirty days after termination or expiry to export data it remains authorized to receive. This right does not require buying a new subscription. Secure assistance may replace ordinary access where needed. A revoked consultant cannot use export to obtain an employer's records without authority. Employer rights and lawful retention duties continue under the employer's own agreement.

5 Changes and notices

The Terms state the order of precedence and the process for changes. This Home Agreement and Rider govern the named-consultant service and its commercial rules; the Order supplies the permitted customer-specific quantity, amounts and dates. The DPA governs processing matters. Other SafeGora terms are not incorporated unless this Agreement names them.

A later public price or policy does not silently change an accepted Order. Changes follow the required notice and any affirmative acceptance required under the Terms. Ordinary monthly renewal at the already accepted price and quantity does not require a new monthly checkbox. Send contractual, billing, cancellation and refund inquiries to Ollie@safegora.com. The firm's contact details are those recorded in its Order or validly updated afterward.

Named Seat Rider

Version 2026-10-23.4

R1 Named licenses

One license covers one identified active person in the firm. Active firm administrators count. The same person is counted once across the firm's client workspaces; copies of that person's account in client workspaces do not create extra licenses. Purchased but unassigned licenses remain billable.

The firm must keep its roster accurate and use separate individual accounts. It may deactivate a person and reassign that license to another person for a legitimate staffing change. Shared logins or rotating simultaneous users to avoid purchasing their licenses are not permitted. Reassignment alone does not change the purchased quantity or create a refund.

R2 Free trial

The trial lasts thirty consecutive days and allows up to ten named consultants without requiring a card. It begins when the firm's workspace is approved and its initial setup is complete. Billing shows the actual trial dates. It does not wait for the first login, receipt of an email, a client's invitation or the first client engagement. Waiting for client access uses trial time. The trial does not pause, restart or extend because a user changes, a card is saved or a payment is retried.

Trial expiry alone creates no paid subscription charge. If the firm does not expressly choose paid service, its ordinary trial access ends at the displayed expiry, subject to the separate record-return and billing rights in the Agreement.

R3 Choosing paid service

The price is USD 79 per purchased named consultant per month, billed in advance, plus applicable tax. There is no firm base fee or annual plan under this offer. It creates no separate setup, professional-service, AI, usage or processing surcharge.

The initial paid quantity is any supported positive whole number shown in the reviewed Order. It may be below or above ten. Before choosing a lower quantity, the firm must deactivate enough users so its active roster fits. The trial's ten-person allowance does not become a minimum paid purchase.

Before payment authorization, billing shows the quantity, unit price, monthly subtotal, applicable tax, amount due, payment method, charge timing and renewal terms. The authorized firm payer must affirmatively accept the paid Order and recurring charges. Saving or changing a payment method alone is insufficient. An expired or materially changed review requires a fresh review and acceptance.

During an unexpired trial, the default paid election schedules the first charge for the displayed trial end. The firm may instead expressly choose to end the trial early and accept the reviewed immediate charge. In that case, unused free days are given up only when payment and paid service are confirmed; the purchased allowance then replaces the trial allowance. After trial expiry, a new accepted purchase charges at the disclosed time without backdating charges to the intervening gap or restarting the trial.

Paid access begins after payment is confirmed. While a purchase is being confirmed, keep the active roster within the quantity accepted; a pending purchase does not add trial licenses. If payment needs authentication, fails or remains uncertain, follow the displayed instructions or contact support. Retrying payment does not itself promise a new full billing month or move the invoice's billing dates. The recorded Order, actual invoice period and applicable correction rights govern.

R4 Renewal and quantity changes

The subscription renews monthly at the accepted USD 79 unit price and current accepted quantity, plus applicable tax, until changed or canceled under the Agreement.

An eligible active subscription can increase or decrease its quantity through a reviewed billing change. The administrator must accept the displayed immediate amount, new quantity and renewal subtotal. An increase charges the reviewed prorated amount for the remaining period. Additional licenses become available after payment and the change are confirmed. The new monthly subtotal applies to later renewals.

For a decrease, remove enough active users first. The lower license allowance applies when the change is confirmed; the lower monthly subtotal begins at the next renewal. There is no current-month refund or credit merely for the reduction. While a decrease is awaiting confirmation, the firm cannot add users above the requested lower limit.

Only one accepted change can be awaiting confirmation at a time. Changes may be unavailable while payment needs attention, cancellation is scheduled, another change is pending or the next renewal is being processed. Resolve the displayed issue and obtain a fresh review. A requested change does not authorize a different amount if payment details or the quoted total change.

R5 Payments, cancellation and refunds

Tax is calculated for each invoice under the disclosed tax treatment. The firm must keep its billing address and payment method current. Failed payments may be retried for an existing authorized obligation; they do not authorize a different subscription or duplicate charge. Temporary payment-recovery access is not a new trial or a promise of a fixed grace period.

The firm may cancel through billing or an authorized email to Ollie@safegora.com. A request submitted through billing, or correctly emailed before renewal without a delivery-failure notice, is timely and prevents that renewal. The Terms define the deadline. Ordinary cancellation preserves paid-through access, subject to other valid grounds in the Terms. A scheduled first charge may be canceled before collection on the same basis. If a pending license change prevents using an app cancellation or payment-update control, contact support. An authorized cancellation email takes effect when sent before the deadline without a delivery-failure notice; processing or reasonable verification does not postpone it.

Cancellation does not erase a legitimate amount already due. Ordinary current-month fees are not refundable for reduced use, unassigned seats or cancellation, subject to billing corrections, mandatory rights and the Agreement's express remedies. The Refund and Cancellation Policy gives the complete rules. Earlier Orders and acceptance records remain evidence of their original transactions and are not rewritten by this Rider.

SafeGora Named Consultant Terms of Service

Document identifier sg-consultant-terms

Version 2026-10-23.4

Effective Date October 23, 2026

1 Definitions and agreement

“SafeGora” means OllieLabs LLC. “Customer” or “Firm” means the business consulting firm named in the accepted order. “Services” means the SafeGora software and functions included in that order. “Order” means the retained record of the Customer, selected subscription, price, quantity, payment timing and accepted documents. “Customer Data” means information supplied by or for Customer or processed for it through the Services. “Employer” means a client organization that controls its own workplace records. “DPA” means the accepted Data Processing Addendum, its standard processing description in Annex A, and any validly agreed supplement. “Customer Cause” means Customer’s uncured material breach under section 10, a breach of section 4 that justifies restriction under section 10, or a prohibited transaction under section 16.

The Agreement comprises the Order, Named Consultant Home Agreement and Named Seat Rider, these Terms, DPA, Privacy Notice, and Refund and Cancellation Policy, each at the identified accepted version. Their express commitments are contractual; privacy acknowledgment does not authorize unspecified optional processing. Mandatory law prevails. Otherwise, conflicts are resolved in this order: a signed amendment, for its identified subject; the DPA, for processing matters; the Privacy Notice, for its express privacy commitments; the Home Agreement and Rider, for service-specific terms; the Order, for permitted customer-specific selections; these Terms; and then the Refund Policy. A purchase-order boilerplate does not amend the Agreement.

2 Acceptance and existing customers

An authorized representative must affirmatively accept the identified documents after an opportunity to review and retain them. The representative confirms authority to bind Customer. An application, invitation, site visit or saved payment method alone is not agreement to a purchase. Customer receives a retained acceptance record and paid-order confirmation. Different terms or economics cannot be accepted using a stale confirmation.

This version applies only through valid acceptance or amendment. Publication does not replace an existing trial, subscription, employer agreement or commission arrangement. Existing rights and properly incurred obligations remain governed by their applicable agreements. No individual gives a personal guarantee merely by accepting for Customer. This offer is available only to firms established in the United States. SafeGora may decline an application or end a trial if this condition is not met.

3 Access and permitted client work

SafeGora grants Customer a nonexclusive right to use the Services during its trial, subscription and expressly authorized recovery or export period. Named consultants are identified humans active in the Firm workspace or consultant roster. Active administrators count; duplicate representations of the same person within the Firm count once. Client-workspace copies alone do not add seats. Customer may reassign a seat after deactivation, but may not share credentials or rotate simultaneous users to evade capacity limits.

Customer may perform consulting work within each Employer’s actual access grant and the user’s permitted role. Seat payment provides no client access, filing authority or certification authority. Employers retain control of their records and responsibility for required review, submission, posting and retention. Revocation ends corresponding consultant access without deleting the Employer’s records or lawful audit history. Client subscriptions and commissions remain separate.

4 Customer responsibilities

Customer must maintain accurate contacts, protect individual credentials, promptly remove departing users, report suspected unauthorized access, and provide lawful instructions and necessary notices and permissions. It is responsible for its authorized users' conduct, except to the extent caused by SafeGora's breach.

Customer must not bypass access or billing controls, introduce malicious code, materially disrupt others, infringe rights, upload information without authority, resell employer accounts or copy protected software to build a competing product. Independent development and lawful use of Customer's own information remain permitted. Customer must not reverse engineer the Services except where applicable law permits it despite this restriction. When using AI features, Customer and its users must also comply with the Google Generative AI Prohibited Use Policy (policies.google.com/terms/generative-ai/use-policy).

5 Trial and initial payment

The named-consultant offer is USD 79 per purchased seat per month, plus applicable tax, billed in advance. The trial allows up to ten consultants for thirty consecutive days beginning when the Firm workspace is approved and its initial setup is complete, with displayed start and expiry. No card is required. Waiting for client access does not pause or restart it.

A paid subscription requires an authorized payer's affirmative acceptance of the actual quantity, first total, timing, renewal and recurring-payment authorization. Saving a card does not elect payment. Default conversion occurs at the disclosed trial expiry. If offered, an expressly selected "Convert now" election charges the reviewed amount immediately and ends the remaining free trial when paid service is confirmed. A purchase after expiry begins at the disclosed time without retroactive gap charges or a new trial.

The active roster must fit the selected positive whole paid quantity. A reviewed initial purchase may exceed ten. SafeGora will not silently bill all trial seats or increase quantity to match the roster. Paid capacity requires confirmed payment or an expressly agreed settlement. An uncertain payment outcome must be reconciled before another attempt can create a duplicate charge.

6 Renewals, quantity changes and cancellation

The subscription renews monthly at the accepted quantity and USD 79 unit price, plus tax under the disclosed rule, until valid cancellation or change. Unassigned purchased seats remain billable. Invoices identify charges and tax; a changed first-payment total requires renewed review.

Quantity changes require an authorized administrator's review and affirmative acceptance of the new quantity, immediate amount and future recurring total. Increases charge the reviewed time-prorated amount; additional capacity starts only after successful confirmation of the required payment. Remove enough users before requesting a decrease; the lower allowance applies when confirmed, and users cannot be added above the requested limit while confirmation is pending. Decreases provide no current-period refund or credit and reduce the next renewal subtotal. A pending change must be resolved before another takes effect. No informal account edit creates payment authorization.

Customer may cancel using the billing control or an authorized email to Ollie@safegora.com. A request submitted through the control, or correctly emailed before renewal without a delivery-failure notice, is timely and prevents that renewal. The deadline is the renewal time shown in billing or, if none is shown, 11:59 p.m. Pacific Time on the day before the renewal date. Paid-through access remains available, subject to independent lawful suspension grounds. If controls are temporarily unavailable during a pending change, email remains available; processing delay or reasonable verification must not defeat a timely legitimate request. A scheduled first charge may be canceled before collection on the same basis.

Ordinary cancellation, unused seats or reduced use does not refund the current period. Billing corrections, mandatory rights and express termination remedies remain available. Failed payments permit lawful retries of

the authorized obligation, not duplicate subscriptions or new quantities. No fixed recovery grace, late fee or interest is promised. Card replacement cannot supply missing acceptance or release an unauthorized charge.

If a renewal payment is not collected within 10 days after its due date, SafeGora may suspend access, other than billing and export access, after notice. SafeGora may end the subscription if payment remains outstanding at the next renewal date. The cure period in section 10 does not require SafeGora to provide unpaid service.

7 Ownership, license and AI features

SafeGora and its licensors own the Services. Customer and relevant rights holders retain Customer Data rights. Customer grants the limited rights needed to host, reproduce, transmit, adapt and process Customer Data to deliver, maintain, secure and support the agreed functions, including enabled AI functions, through the providers and purposes described in the DPA and Privacy Notice. This does not authorize unrelated sale, advertising or an undisclosed processing purpose. SafeGora may also use Customer Data to maintain and improve the Services, but not to train generative models or build profiles, and may use aggregated or de-identified data that does not identify Customer, an Employer or any individual. Employer records do not become the consultant's property.

AI functions, when made available and enabled for Customer, may transmit relevant inputs and context to the disclosed provider and return generated output. Acceptance of this Agreement does not by itself activate an AI feature. Actual retention and permitted provider uses depend on the identified service, account, settings and agreements; these Terms make no zero-retention promise, and the DPA limits provider training. A new purpose or provider use must comply with the DPA, Privacy Notice and applicable consent requirements.

Customer-enabled integrations. If an authorized user connects the Services to a third-party AI host or other integration, SafeGora will send that host the permitted results the user requests. Those results may contain Customer Data. The host acts under its own terms with Customer or the user and is not SafeGora's subprocessor. Customer must ensure that each affected Employer has authorized that disclosure. Disconnecting stops further disclosure but does not recall information already sent.

Outputs can be inaccurate, incomplete, nonunique or subject to others' rights. Customer must review them before relying on, filing or sharing them. No output is a legal opinion, regulatory certification or substitute for professional judgment. No AI-output intellectual-property indemnity or upstream-provider indemnity is promised. Customer grants SafeGora a perpetual, irrevocable, worldwide, royalty-free license to use and incorporate any suggestions or other feedback about the Services (Feedback) without obligation. Feedback does not include Customer Data, and confidential or personal information remains protected by the Agreement.

8 Privacy, security and verification

SafeGora will comply with the accepted DPA and Privacy Notice, follow lawful documented processing instructions, and maintain their agreed safeguards. Actual roles and applicable law govern; neither a subscription label nor this Agreement executes missing transfer clauses or a business associate agreement. Do not supply HIPAA-regulated information requiring an unexecuted BAA. Employment injury facts are not automatically HIPAA PHI; their source, role and purpose must be assessed.

Verification begins with available reports and reasonable written responses, without implying a certification exists. If insufficient, Customer may seek proportionate additional review under the DPA. Ordinary reviews may be coordinated annually; material incidents, credible noncompliance and regulatory requirements permit additional review. Customer ordinarily bears its auditor's costs and reasonable incremental assistance costs agreed beforehand; SafeGora bears reasonable verification and remediation costs where material noncompliance is established. No report-only condition, fee or scheduling rule may obstruct mandatory audit rights, a regulator or required assistance.

9 Confidentiality

Each party will protect information reasonably understood to be confidential with reasonable care, use it only for the Agreement's purposes, and disclose it only to people needing it who are bound by appropriate duties. Customer Data is confidential. Information independently developed, lawfully obtained without restriction, already lawfully known, or made public without breach is excluded.

Legally required disclosure must be limited and, where lawful, preceded by notice and reasonable cooperation. Protected reporting, regulator communications and legal advice remain allowed. Return, deletion and permitted protected retention follow the DPA. Confidentiality continues while information remains confidential; it does not authorize indefinite retention.

10 Service commitments and remedies

Each party has authority to enter the Agreement. SafeGora will perform its express service, processing and security commitments. Except for those commitments and nonwaivable rights, Services are provided "as is" and "as available," without implied warranties of merchantability, fitness or noninfringement. There is no guaranteed uptime, response time or recovery objective unless a separately accepted SLA expressly provides one. These disclaimers do not remove express refunds, indemnities or return-of-data duties.

Either party may terminate the Agreement for a material breach that remains uncured thirty days after reasonably detailed notice. Immediate proportionate restriction is permitted for an imminent security threat, unlawful access, serious harm or binding legal requirement, with notice where practicable and lawful, and restoration when justified. Payment suspension cannot independently remove previously paid-through rights.

SafeGora may decline renewal on at least thirty days' notice. Unused prepaid fees are refundable after Customer validly terminates for SafeGora's uncured material breach, SafeGora ends paid service early without Customer Cause, an incurable covered IP claim causes termination, or the DPA permits termination for an unresolved reasonable subprocessor objection. These agreed remedies need no additional discretionary approval. For this indivisible subscription, refund the net prepaid fee multiplied by the actual unused fraction of the period, correct tax, and deduct prior credits or refunds for the same amount.

11 Ending service and records

Ordinary access ends at expiry or termination, but Customer retains billing and evidence access and at least thirty days to export information it is entitled to receive, through a secure assisted method where necessary. A new paid subscription is not required for that return right. A revoked consultant cannot export Employer records without renewed authority; the Employer's contract and custodianship continue.

Working-copy deletion, backups, infrastructure audit records and legal holds follow the actual retention categories and periods in the DPA and Privacy Notice. A shorter application-log period does not override a separately disclosed provider-required audit period. Retained copies remain restricted; Customer's own statutory retention duties continue. Accrued payment, confidentiality, ownership, dispute and applicable processing obligations survive as necessary.

12 Indemnities

SafeGora will defend a third-party claim that its unmodified software or documentation, used as permitted, infringes intellectual-property rights, and pay covered final judgments or approved settlements. Customer will provide the same protection for a third-party claim that Customer-supplied content infringes those rights. Customer will also defend SafeGora against a third-party claim arising from (a) Customer Data that Customer or its users supplied without the authority, notices or permissions required by law or by the applicable Employer, or (b) use of the Services in breach of section 4, and will pay covered final judgments or approved settlements. These obligations are subject to section 13 and include reasonable defense costs within its applicable cap. They do not cover AI-generated outputs merely because the output was generated through the Services.

Coverage excludes a claim to the extent caused by the protected party's unauthorized modification, prohibited use or combination where infringement would not otherwise occur. Customer's indemnities do not cover SafeGora's use outside lawful instructions. Prompt notice is required, but delay excuses performance only to the extent materially prejudiced. The defending party controls a competent defense, keeps the other informed and pays reasonable cooperation costs. Settlement requires consent if it admits the protected party's fault, imposes nonmonetary duties or lacks a full release. Consent must not be unreasonably withheld.

SafeGora may procure continued use or provide materially equivalent noninfringing software. If neither is reasonably available, it may terminate affected service and provide the section 10 refund. A failure to provide a required defense permits reasonable self-defense and recovery within the same coverage and cap.

13 Liability allocation

"Annual Fees" means fees paid or properly payable for the Services in the twelve months before the event giving rise to the claim; related events are treated together. Each party's ordinary aggregate liability under the Agreement is limited to Annual Fees. Covered IP indemnities have a cap equal to the greater of Annual Fees or USD 100,000. Claims caused by breach of security, privacy, data-processing or confidentiality duties have a cap equal to the greater of three times Annual Fees or USD 250,000.

These limits do not stack. For all capped claims combined, recovery cannot exceed the highest applicable cap, and each category remains subject to its own limit. Defense costs, judgments and settlements reduce the applicable aggregate. Different labels, legal theories or indemnity claims do not multiply recovery. Ordinary Annual Fees may be zero during a free trial; during a trial with no Annual Fees, the IP and security/privacy/confidentiality caps are USD 10,000 each instead of the USD 100,000 and USD 250,000 floors.

Neither party is liable for indirect, special, consequential or punitive damages or lost profits or goodwill. This exclusion does not prevent covered third-party judgments and settlements under section 12, or reasonable direct incident investigation, notification, containment and restoration costs caused by breach of the duties subject to the higher security/privacy/confidentiality cap.

The caps and the exclusion of indirect damages in this section do not apply to fraud, willful misconduct or liability that law prohibits limiting. Properly due payment obligations, billing corrections and express refunds remain payable. No term limits a regulator's powers or a person's nonwaivable rights. There is no duplicate recovery for the same loss.

14 Notices and changes

Ordinary contractual notices use Ollie@safegora.com and Customer's designated account contacts. Unless earlier delivery is established, a properly addressed email is deemed received the next business day after sending if no failure notice is returned and the sender has no reason to know delivery failed. Mandatory notice and service-of-process rules prevail. Billing cancellation instead uses section 6's sending-before-deadline rule, without an added business-day delay.

Material prospective amendments require at least thirty days' direct notice identifying the changes, version, effective date and cancellation option; longer required periods apply. Current-period rights and accrued claims are preserved. Price or quantity changes, expanded data uses requiring consent, or changes to liability limits or dispute resolution require affirmative acceptance. For other changes, continued use after clear notice and the effective date constitutes acceptance only where law permits. A page edit alone is insufficient. If a change is not accepted, the existing Agreement continues until valid cancellation, nonrenewal or termination; no changed charge is collected without authority.

15 Governing law, disputes and claims period

Before starting arbitration or court proceedings, a party must send a written description of the dispute, and the parties must try in good faith to resolve it for 30 days. This does not prevent interim relief or cause a claim to expire.

Oregon law governs, without regard to its conflict-of-laws rules and subject to nonwaivable law; the Federal Arbitration Act applies where applicable. Disputes arising out of or relating to the Agreement are resolved by individual binding AAA arbitration under its Commercial Rules applicable when filed, in English before one arbitrator, seated in Portland, Oregon, or with agreed remote hearings. The procedural rules and fees are available at adr.org/rules-forms-and-fees/commercial/. They do not amend substantive contract rights. Judgment may be entered by a competent court.

No class arbitration is agreed. Courts decide formation and enforceability of that restriction. Nonwaivable representative remedies, regulatory complaints and claims that cannot lawfully be arbitrated remain available. Either party may seek interim court protection for confidential information, data or intellectual property. Nonarbitrable disputes belong in the state courts located in Washington County, Oregon, or the federal courts for the District of Oregon, unless mandatory law requires otherwise. Either party may instead bring an individual claim in a small-claims court with jurisdiction. For any claim that proceeds in court, each party waives trial by jury where law permits.

Ordinary contractual claims between the parties must be commenced within two years after legal accrual. This does not shorten nonwaivable or statutory privacy rights, bar claims for fraud or concealed wrongdoing, displace applicable tolling, or start an indemnity claim's period before it legally accrues. An unenforceable restriction yields to the applicable statutory period.

16 General provisions

Each party must comply with applicable export-control and sanctions law; neither must perform a prohibited transaction. SafeGora may conduct reasonable checks and proportionately restrict prohibited use.

Neither party may assign without consent, not unreasonably withheld, except to a business successor that assumes the obligations on notice and satisfies applicable processing restrictions. Events beyond reasonable control excuse affected performance only while reasonably mitigated; they do not erase payment already due or mandatory remedies. The parties are independent contractors. Sever invalid provisions only as law permits. A waiver must be attributable to its giver. This Agreement supersedes proposals about its own Order, not independent Employer, historical or commission contracts.

There are no third-party beneficiaries. Employers, workers and other individuals cannot enforce the Agreement, but their nonwaivable statutory rights are unaffected. Subject to the preceding exclusions, the Agreement is the parties' entire agreement about its Order and supersedes prior proposals and understandings about it. It may be accepted electronically and executed in counterparts. "Including" means "including without limitation", and headings do not affect interpretation.

SafeGora Named Consultant Privacy Notice

Document identifier sg-consultant-privacy

Version 2026-10-23.4

Effective Date October 23, 2026

1 Who we are and what this notice covers

OllieLabs LLC, operating as SafeGora, provides the named-consultant service to business consulting firms. This notice covers the firm's account, checkout, workspace and related support. Our contact is Ollie@safegora.com. Our postal address is 3400 NE John Olsen Ave, Ste 200, Hillsboro, OR 97124, United States.

The firm is the Customer identified in the accepted Order. Capitalized terms have the meanings in the Terms of Service or Data Processing Addendum (DPA). The Home Agreement incorporates this version's privacy commitments into the Agreement. The DPA controls our processing of Customer Personal Data on the Customer's behalf. This notice also describes information we use for our own account administration, security, billing and measurement purposes; those activities do not automatically have the same legal role as processing workplace records for a Customer.

The employer controls its workplace records. A consultant's subscription does not itself authorize access to those records. The actual employer permission and applicable law determine what the consultant may do. This notice describes the named-consultant service and does not replace notices provided for separate public marketing activities. Its commitments continue to apply to information processed for the named-consultant service.

2 Information and purposes

Information	Main purposes
Names, business contact details, firm identity, account roles, login and session information	Create and administer accounts, authenticate users, manage permissions, provide support and send service notices.
Workplace records supplied or accessed through authorized features, including observations, incident narratives, actions, attachments, photographs and relevant worker or client details	Store, organize, search, display, analyze and export records for the Customer's authorized work. Some enabled features use AI as described below.
Prompts, selected record context, retrieval queries, images or other supported inputs, and generated results	Provide AI assistance, retrieval, drafting and related features; maintain their security and reliability.
Orders, subscription quantities, invoices, payment status and payment-method references	Process subscriptions, collect authorized payments, manage changes and refunds, and retain necessary accounting evidence. Payment providers separately handle payment credentials.
Support correspondence and request records	Resolve issues, verify authority, respond to rights requests and maintain evidence of our response.

Information	Main purposes
IP addresses, browser and device details, request and event metadata, consent choices and usage information	Operate and secure the service, troubleshoot failures, measure use and, where applicable, measure advertising and purchases.

We collect information from users, their firm and authorized employers, from service activity and devices, and from providers involved in account, payment or service delivery. Health-related workplace information can be sensitive even when it is an employment record. Submit only information necessary for an authorized purpose. Do not submit information requiring a HIPAA business associate agreement unless that agreement is in place for the proposed use.

3 AI processing

When AI features are made available and enabled for the Customer, consulting workflows may use Google Gemini for assistance such as questions about portfolios, field-note analysis, visit-report drafting and retrieval. Requests can include the user's question and relevant client, site, engagement, visit or workplace context. Visit-report features can send photographs as well as text. Retrieval can send a query for embedding, which converts text into a representation used to find related material. AI processing can occur within a workflow; it is not limited to a separate chat window.

Automated minimization or redaction is not a guarantee that inputs contain no personal or confidential information. AI results can be inaccurate or incomplete. An authorized person must review them before relying on them or communicating them as professional findings. The Terms explain the responsibility for that review.

The Google service used matters. Google Cloud Vertex AI and the Gemini Developer API have different contractual and operational conditions. The service can use Vertex AI or a separately configured Gemini API connection. Annex C to the DPA identifies these provider services. A global AI endpoint does not promise that processing remains in the main application's hosting region.

Our Agreement does not grant SafeGora a general right to train foundation models on Customer Data. We must use processing arrangements consistent with the DPA. This is not a promise that every Google product has identical training restrictions, that all AI requests have zero retention, or that no provider personnel can ever review data for safety or legal purposes. Provider retention, caching, abuse monitoring and any permitted review depend on the service, settings and applicable agreement. SafeGora will send Customer Data only to AI services offered under paid terms that prohibit the provider from using it to train or improve the provider's models. It will not send Customer Data to a connection subject to Google's Unpaid Services data-use terms. Before sending Customer Data to an AI service, SafeGora will verify that the provider service, account terms and configuration meet this restriction.

4 Service providers and other disclosures

Our service providers include Google Cloud and Google AI services, WorkOS for identity, Stripe for payments, Google Workspace for transactional email, and Cloudflare for DNS and any configured edge services. The DPA's provider schedule describes their service roles. Google Analytics and Google Ads have separate measurement and advertising roles described below; they are not automatically treated as subprocessors for every purpose. If an authorized user connects SafeGora to a third-party AI host, such as ChatGPT or Claude, that host receives the permitted results the user requests, which may include Customer Data. The host processes those results under its own terms with the Customer or user and is not SafeGora's subprocessor. The Customer must have each affected employer's authorization for the disclosure. Disconnecting stops further disclosure but does not recall information already sent. Section 7 of the Terms governs these customer-enabled integrations.

We may disclose information to authorized firm or employer users, to providers needed for the relevant service, in response to lawful compulsory process, to protect rights and investigate abuse where permitted, and in a business transfer subject to applicable protections. We may also disclose information when the person with authority instructs us to do so. A provider's separate account, fraud-prevention, payment or advertising purposes are governed by the terms and legal roles applicable to that activity.

5 Analytics, advertising and browser storage

We also collect first-party operational and product telemetry, including navigation events, to operate, diagnose and improve the service. This processing is separate from Google Analytics and advertising measurement.

When Google Analytics is configured, the platform can load Google's tag on account, checkout and signed-in service pages. Some service events, including AI feature events, are sent to the analytics interface. Available payment-return flows can also report a purchase conversion through the Google Ads interface. Whether a particular event reaches a configured Google destination depends on the page, configuration and consent state.

Loading a Google script makes a request to Google. Google may receive connection and browser metadata such as an IP address and user-agent. A denied cookie-consent state does not necessarily prevent that request or every subsequent signal: Google's advanced consent mode can send signals without analytics or advertising cookies. This notice makes no blanket promise of no Google requests on signed-in pages, no measurement before consent, or universal IP anonymization.

Depending on the event and configuration, measurement can include page or referrer information, event details, consent state, and purchase value, currency or transaction identifiers. Analytics and advertising cookies or identifiers are subject to the applicable consent choices and law. Necessary session, authentication, security and preference storage supports the service independently of optional measurement.

Use the consent controls offered on the relevant page to change available choices. A choice made on a public page may be carried to the platform through shared preference storage. You can also contact us about an opt-out or consent concern. We must respect legally applicable opt-out preference signals and consent requirements. Advertising disclosures may be a sale or sharing of personal information under applicable privacy law even when no money is paid for the information. The applicable opt-out rights remain available; accepting the business Agreement does not waive them.

6 Retention

Retention differs by record type. There is no single 90-day maximum covering all service, security, audit, backup or provider records.

Record type	Retention basis
Customer workplace and service records	The service relationship, authorized Customer or employer instructions, applicable recordkeeping duties, and the return and deletion provisions in DPA section 9. The Customer has at least 30 days after termination or expiry to request an authorized export.
Ordinary application and edge logs	The applicable configured retention period and the time reasonably needed to operate, diagnose and secure the service. A separate incident or legal preservation need can require a longer period.
Google Cloud required audit logs	Google retains the logs in its required audit bucket for 400 days. SafeGora cannot shorten that bucket's retention. Copies exported elsewhere have separate retention rules.
Orders, payments, tax, acceptance and dispute records	The period reasonably needed to perform the Agreement, meet applicable accounting or legal obligations and resolve actual claims. These records are distinct from a consultant's right to access employer data.

Record type	Retention basis
Support, inquiry, consent and rights-request records	The time reasonably needed to resolve the matter, record consent or withdrawal, honor an opt-out and meet applicable accountability requirements.
AI provider records, analytics records and backups	The applicable provider service and settings, the purpose of the record, and relevant contractual or legal obligations. An application's log-deletion rule does not delete every provider copy or backup.

We must not retain personal information indefinitely merely because it is convenient. We must review continuing needs and delete or de-identify information when it is no longer needed, subject to lawful retention and the DPA. Contact us for the retention information applicable to a particular record or request. Employer records may remain subject to the employer's separate agreement and legal duties after a consultant loses access.

7 Locations and safeguards

Our published primary application hosting region is Google Cloud us-west1 in the United States. That is not an assurance that all providers, AI requests, support operations, logs or backups stay in that region or solely in the United States. Google AI global endpoints and providers' international operations can involve other countries. The DPA governs required safeguards for Customer Personal Data. Any legally required international-transfer instrument must be in place and apply to the relevant transfer before it occurs.

We must maintain the reasonable technical and organizational safeguards specified in the DPA. This notice does not claim a SafeGora SOC 2 or ISO certification, universal multifactor authentication, uninterrupted availability or a guaranteed recovery time.

8 Rights and contact

Depending on applicable law, individuals may have rights to know or access information, correct it, request deletion or portability, withdraw consent, object to or restrict processing, opt out of sale, sharing or targeted advertising, limit certain sensitive-data uses, appeal a decision or complain to a regulator. We will not unlawfully discriminate against someone for exercising a right.

Send requests to Ollie@safegora.com. We may need proportionate information to verify the requester and their authority. When we process workplace records for a Customer or employer, we will direct the request to the responsible organization and assist as the DPA requires. We will respond within the applicable legal deadline. A consultant cannot obtain an employer's records through a privacy request without the necessary authority.

9 Changes

The accepted version's contractual commitments change only under the Agreement's change rules. We will give the required notice of prospective material changes and obtain affirmative acceptance or consent where the Agreement or law requires it. A newer privacy page does not retroactively authorize a different use of previously collected information.

SafeGora Named Consultant Refund and Cancellation Policy

Document identifier sg-consultant-refund

Version 2026-10-23.4

Effective Date October 23, 2026

1 Application

This policy covers the monthly named-consultant subscription supplied by OllieLabs LLC, operating as SafeGora, when the firm's accepted Order identifies it. It is for New Firms, as defined in the Home Agreement, including their later paid elections and accepted quantity changes. Existing subscriptions, trials, historical partner plans and earlier transactions keep their applicable terms. A refund request's date does not substitute a later policy or remove accrued rights.

The price is USD 79 per purchased named consultant per month, plus applicable tax, billed in advance. No annual plan or annual refund window applies. This offer creates no separate setup, AI, usage, professional-service or processing surcharge, commission payment or SLA credit.

2 Trial and paid election

The thirty-day, ten-consultant trial requires no card. It starts when the firm workspace is approved and initial setup is complete; billing shows the dates. Client-access delays, payment setup and retries do not restart it. Trial expiry and saving a card do not authorize paid charges.

A paid purchase requires the firm's affirmative acceptance of the reviewed amount, quantity, timing and monthly renewal. During trial, the default first charge is at the displayed expiry. An expressly chosen early purchase charges now; unused free days are forfeited only when payment and paid service are confirmed. After expiry, a new purchase is not backdated to the gap. There is no monetary refund for uncharged free days. Later payment of an existing valid invoice does not automatically restart its billing period.

3 Quantity changes

An accepted increase charges the reviewed prorated amount now; added licenses become available after payment and confirmation. An accepted decrease requires the active roster to fit the lower quantity. The lower allowance applies when confirmed, and the lower monthly subtotal starts at the next renewal. It creates no current-month refund or credit. Reassignment and unused licenses do not themselves reduce the purchased quantity. A pending decrease prevents adding users above its requested limit.

4 Cancellation

Request cancellation through billing or an authorized email to Ollie@safegora.com. A request submitted through billing, or correctly emailed before renewal without a delivery-failure notice, is timely and prevents that renewal. The Terms define the deadline. Ordinary cancellation ends the subscription at the current paid period's end. Paid-through access remains, subject to other valid grounds in the Terms. A scheduled first charge may be canceled before collection on the same basis.

If a pending change prevents app cancellation, email remains available. An authorized cancellation email takes effect when sent before the deadline without a delivery-failure notice; processing or reasonable verification does not postpone it. SafeGora will correct an erroneous charge collected despite a timely legitimate cancellation. Cancellation does not settle legitimate unpaid invoices or authorize a duplicate charge.

5 Ordinary refunds and protected exceptions

Properly authorized current-month fees are ordinarily not refundable because the firm cancels, uses fewer licenses, leaves seats unassigned or waits for client access. Mandatory rights, unauthorized charges, billing errors, duplicate charges and express contractual remedies remain protected.

Refunds promised in the accepted Home Agreement, Terms or DPA are entitlements when their conditions are met; they require no additional discretionary approval. These include the applicable remedies for SafeGora's uncured material breach, early termination without Customer Cause, as defined in the Terms, an unresolved covered intellectual-property claim, or an unresolved reasonable subprocessor objection under the DPA.

Unless a later valid agreement expressly prices a separate affected component, the affected service is the whole named-consultant subscription. Its covered termination refunds net prepaid fees multiplied by the actual unused fraction of that paid period, with applicable tax correction. Prior refunds and credits are counted to prevent double recovery. This termination remedy differs from an ordinary quantity decrease. SafeGora may also grant an additional exception without making that exception universal.

6 Requests and payment

Email Ollie@safegora.com with the firm account, invoice or Order reference, and reason for the request. Do not send complete card details. SafeGora will check the accepted terms and payment record, explain the outcome, and return amounts owed through the original payment method where practicable, with another lawful arrangement if necessary. Processor and bank settlement times vary; this policy promises no fixed payment date. Mandatory deadlines and remedies prevail. Any material future change follows the notice and acceptance rules in the Terms and does not rewrite an earlier transaction.

SafeGora Named Consultant Data Processing Addendum

Document identifier sg-consultant-dpa

Version 2026-10-23.4

Effective Date October 23, 2026

1 Application and standard schedule

This Data Processing Addendum (DPA) forms part of the Agreement between OllieLabs LLC, operating as SafeGora, and the Customer identified in the accepted Order. It governs personal information SafeGora processes on the Customer's behalf through the named-consultant service (Customer Personal Data).

Annex A supplies the standard processing description for this offer. It applies when the Agreement is accepted; no separate customer questionnaire is required for that standard description. The Customer's identity and contact details are incorporated from the Order and maintained account details. An agreed supplement is needed only for a material use outside the standard description or where applicable law requires additional terms.

The Customer is a controller or business for data it controls. Where it acts for an employer as a processor or service provider, it must have authority to appoint SafeGora as a further processor and give the relevant instructions. SafeGora's role follows the actual processing, authority and law. Neither this DPA nor payment creates an employer's permission or transfers ownership of employer records.

SafeGora separately determines the purposes of certain account administration, payment, fraud-prevention and measurement activities described in the Privacy Notice. Calling those activities separate does not permit SafeGora to repurpose Customer Personal Data contrary to this DPA or override the role required by law.

2 Instructions and permitted use

The Agreement, the standard schedule, the Customer's authorized configuration and feature use, and lawful written directions are the Customer's documented instructions. SafeGora may process Customer Personal Data only to provide the agreed service, maintain its security and reliability, improve the Services as the Terms permit, carry out those instructions, or comply with applicable law. SafeGora will notify the Customer before legally compelled processing unless the law prohibits notice.

A customer-enabled integration described in the Terms is a Customer instruction. A third-party host that receives results through such an integration is not a subprocessor under section 5.

The Customer must provide necessary notices, establish an appropriate legal basis and obtain required permissions for the information and instructions it supplies. SafeGora will tell the Customer if it reasonably believes an instruction violates applicable data-protection law and may pause the affected instruction while the parties resolve it. That pause must be limited to what is reasonably necessary.

Where California service-provider or contractor rules apply, SafeGora will not sell or share Customer Personal Data, retain, use or disclose it outside the specified business purposes or direct business relationship, or combine it with other personal information except as applicable law permits. Where SafeGora acts as a contractor under the California Consumer Privacy Act, it certifies that it understands these restrictions and will comply with them. SafeGora will provide the required level of protection, notify the Customer if it can no longer meet these obligations, and permit reasonable steps to stop and remedy unauthorized use. These restrictions also govern relevant downstream processing. They do not eliminate individuals' statutory rights.

Do not provide data requiring a HIPAA business associate agreement, a government-specific agreement or another special authorization unless that agreement or authorization is in place for the proposed use. Ordinary employment information is not automatically HIPAA-regulated merely because it concerns health; its actual source, holder and use matter. The parties must assess sensitive information and minimize it to the authorized purpose.

3 People, security and incidents

SafeGora will limit access to persons who need it for their duties, require confidentiality obligations, and maintain reasonable technical and organizational measures appropriate to the information and risks, including Annex B. SafeGora remains responsible for its personnel's compliance. The Customer must maintain its user roster and employer permissions and promptly report suspected compromise.

SafeGora will notify the Customer without undue delay after becoming aware of a security breach affecting Customer Personal Data, and meet any shorter applicable legal deadline. The notice will include known facts about the incident, affected information, likely consequences, containment and remediation, and a contact. SafeGora may provide information in stages as the investigation develops. It will take reasonable steps to contain and remedy the incident, preserve relevant evidence and assist the Customer with applicable notification duties. Notice is not an admission of liability.

An unsuccessful attack or blocked attempt that does not compromise Customer Personal Data is not itself a reportable breach under this clause. The parties must not use that distinction to withhold notice of an actual incident. SafeGora will not notify affected individuals on the Customer's behalf without instructions unless law requires it.

4 AI assistance

Where AI assistance and retrieval are made available and enabled for the Customer, the processing described in this section uses the Google services identified in Annex C. Processing may include questions, notes, authorized record context, compliance summaries and photographs used in visit-report drafting, as well as creating embeddings from text. An instruction to use an enabled workflow includes the processing reasonably necessary for that workflow as described in the Agreement; it does not authorize unrelated model development or advertising use of Customer Personal Data.

SafeGora must choose and operate provider services under written terms compatible with this DPA. Provider products may have different data-use terms; the particular service used must satisfy this DPA. SafeGora will send Customer Data only to AI services offered under paid terms that prohibit the provider from using it to train or improve the provider's models. It will not send Customer Data to a connection subject to Google's Unpaid Services data-use terms. Before sending Customer Data to an AI service, SafeGora will verify that the provider service, account terms and configuration meet these requirements. A change to a provider service that materially expands permitted data use requires the notices, agreement and any separate consent required by the Agreement and law.

SafeGora receives no general license to train foundation models on Customer Data. Provider processing may nevertheless involve retention, caching and safety or abuse review under applicable service terms. This DPA does not promise zero provider retention, no possible human review, perfect redaction or a particular physical location for a global endpoint. Provider terms cannot reduce SafeGora's own obligations under this DPA. AI results require the human review described in the Terms.

5 Providers

The Customer generally authorizes the service providers described in Annex C for their stated processing purposes. SafeGora will impose written data-protection obligations appropriate to their role and no less protective of Customer Personal Data than this DPA requires, taking account of the nature of their services. SafeGora remains responsible for a subprocessor's performance of the processing obligations it delegates.

SafeGora will give the Customer at least 30 days' direct notice before adding or replacing a subprocessor or materially expanding a listed subprocessor's processing of Customer Personal Data. Notice must identify the provider, purpose and material location or data-use change. A listing update alone is insufficient notice. The Customer may object during that period on reasonable data-protection grounds.

The parties will try to resolve a reasonable objection through an appropriate alternative, safeguards or removal of the affected processing. SafeGora must not send the Customer's Personal Data to the disputed new processing while a timely reasonable objection remains unresolved. If no reasonable solution is available, either party may terminate the affected service before the change takes effect. The Customer receives the unused prepaid-fee refund specified in the Refund Policy. For this offer, the affected service is the whole subscription unless the parties have separately priced and accepted a distinct component. This agreed refund does not require a further discretionary approval.

6 Assistance and rights

Taking account of the processing and information available to it, SafeGora will reasonably assist the Customer with access, correction, deletion, portability, restriction, objection and other applicable privacy rights; security and incident obligations; legally required assessments; and consultations with regulators. It will promptly forward a request concerning Customer Personal Data unless authorized to respond directly. It may verify the requester's identity and authority proportionately.

The Customer remains responsible for deciding and documenting its lawful response. SafeGora will not disclose employer information to a consultant whose permission has expired or been revoked merely because that person requests an export or exercises an account right. A rights request does not authorize destruction of another organization's lawfully retained records.

7 Transfers

The Customer understands that the primary application region, an AI endpoint and a provider's support locations are different matters. Processing can occur in the locations described in Annex C, including global services. SafeGora will use legally required transfer safeguards for Customer Personal Data. If a particular transfer requires additional standard contractual clauses or another instrument, the parties must put the required instrument and particulars in place before that transfer. This DPA alone does not constitute an executed set of EU standard contractual clauses, a UK addendum or a HIPAA agreement.

8 Information reviews and audits

SafeGora will provide information reasonably necessary to demonstrate compliance with this DPA. The parties will ordinarily begin with current relevant reports, security information and written responses under confidentiality protections. This clause does not represent that SafeGora holds any particular certification or audit report.

If that information is insufficient for a reasonable compliance assessment, the Customer may request a proportionate audit by itself or a qualified independent auditor bound by confidentiality. Ordinarily an audit requires reasonable advance notice, occurs during business hours and is limited to once in twelve months. Additional or urgent review is allowed when reasonably necessary after a relevant incident, credible evidence of material noncompliance, or a regulator's or applicable law's requirement.

The parties will agree a reasonable scope and method that protects other customers, confidential security details and service availability. Intrusive testing of production systems requires advance written agreement unless competent legal authority requires it. SafeGora may offer equally effective evidence or a less disruptive method, but may not use scheduling, cost or confidentiality to frustrate a legally required review or reasonable verification and remediation rights.

The Customer normally pays its own auditor and expenses. Any charge for exceptional assistance beyond ordinary information requests must be reasonable and agreed in advance. SafeGora bears its own remediation costs and, if the review establishes its material breach of this DPA, the reasonable external audit costs attributable to that breach. No additional fee is a condition of meeting a nonwaivable legal obligation.

9 Return, deletion and retention

During the service and for at least 30 days after termination or expiry, the Customer may request a reasonable export of data it remains authorized to receive. SafeGora may use a secure assisted export if ordinary account access would be unsafe. This right does not require a new paid subscription or preserve revoked employer permissions.

After the export period, SafeGora will return or delete Customer Personal Data at the Customer's lawful choice. If the Customer gives no choice, SafeGora will delete it under the documented retention schedule. Retention beyond that is limited to specific legal requirements and narrowly necessary billing, security or dispute records where applicable law and the parties' actual roles permit it. SafeGora must identify the basis, minimize and restrict retained information to that purpose, and delete or lawfully and irreversibly de-identify it when the basis ends. Where applicable processor law permits retention only when law requires storage, that stricter rule controls. Employer records governed by a separate continuing relationship must be handled under that relationship and the employer's lawful instructions.

Backup copies may remain until their scheduled rotation and expiry. They must remain protected and must not be used for ordinary business processing. If restored, applicable deletion instructions and revoked access must be reapplied. SafeGora will provide available information about completion on a reasonable request. Moving information to an archive is not by itself deletion.

Annex D identifies the relevant retention categories. There is no blanket 90-day deletion promise. Google Cloud's required audit bucket has a fixed 400-day retention period, and copies in other destinations are subject to their own applicable schedules. SafeGora must maintain a documented, purpose-limited retention schedule and review it; this DPA does not authorize indefinite retention for convenience.

10 Liability and priority

The Terms' liability provisions, including the separate limit for privacy, security and confidentiality claims and their exceptions, apply to this DPA. They do not restrict a regulator's powers or an individual's nonwaivable rights. Where this DPA conflicts with another part of the Agreement about processing Customer Personal Data, this DPA controls. An executed mandatory transfer instrument controls to the extent it requires. All other conflicts follow the Terms' order of priority.

Annex A Standard processing description

This schedule applies to the ordinary named-consultant offer without a separate customer form.

Particular	Standard description
Parties and contacts	OllieLabs LLC, operating as SafeGora, at the address and email in the Privacy Notice; the Customer and its authorized account contact identified in the accepted Order and account records.
Subject matter	A consulting firm's practice workspace and its users' authorized work with employer clients.
Purposes	Account and permission administration; creating, storing, organizing, searching, displaying, drafting, analyzing and exporting authorized consulting and workplace records; notifications, support, security and service reliability. Enabled AI functions form part of these purposes as described in section 4.
Operations	Collection, recording, storage, retrieval, use, transmission to authorized users or providers, transformation including AI analysis or embeddings where the feature uses them, restriction, return and deletion.

Particular	Standard description
People	Firm users and contacts; employer contacts, workers, contractors, witnesses and other people whose information is lawfully included in authorized workplace records.
Information	Business identifiers and contacts, account roles, employment and site context, observations, incident narratives, corrective actions, relevant photographs or attachments, feature inputs and outputs, and service/audit metadata. Categories are limited by the features and information the Customer actually uses.
Sensitive information	Workplace injury or other sensitive information only when necessary, lawful and within the agreed service. Excluded special uses described in section 2 require the relevant additional agreement. No general permission to upload medical records, identification documents or unrelated sensitive information is implied.
Duration and frequency	During the service as required by authorized feature use, including ongoing storage, and afterward only for the export, return, deletion or justified retention purposes in section 9.
Role and employer authority	The Customer is a controller/business or an authorized processor/service provider according to the actual relationship. Employer permissions identify which client records and actions are authorized; the schedule supplies no missing permission.

Annex B Contractual safeguards

SafeGora will maintain controls appropriate to the service risks: individual user and administrator access; least-privilege and tenant/role restrictions; timely removal of obsolete permissions; confidentiality and appropriate personnel instruction; protection of data in transit and at rest; controlled management of credentials and secrets; vulnerability and change management; relevant security logging and incident response; and reasonable backup and recovery arrangements.

The Customer must protect its credentials and devices, assign appropriate roles, maintain accurate users and client permissions, and avoid unnecessary sensitive information. The parties will cooperate on suspected misuse. These safeguards are contractual obligations. They do not constitute a certification of flawless control operation or a promise of a particular authentication product, encryption suite, uptime or restoration deadline.

Annex C Provider services and locations

The table identifies the provider services within the described offer. A service listed as configuration-dependent is used only when the corresponding configuration or feature applies. SafeGora's obligations in sections 2, 4, 5 and 7 apply in every case.

Provider service	Purpose and information	Location scope
Google Cloud	Application compute, databases, storage, logging, monitoring and related infrastructure; Customer Personal Data and service metadata needed for those functions.	Published primary application region us-west1, United States. Provider support, ancillary services and separate log or backup locations may differ.
Google Gemini through Vertex AI	AI generation and retrieval embeddings; feature inputs, selected customer context, permitted images and generated results.	Text generation can use a global endpoint; the configured embedding implementation uses us-west1. Global processing is not a US-only commitment.

Provider service	Purpose and information	Location scope
Google Gemini Developer API when separately configured	An alternative Google AI connection for the supported functions. The actual project, billing status and applicable data-processing terms determine provider data use.	Google's applicable service locations; no region-specific or zero-retention assurance. Use with Customer Personal Data must meet section 4.
WorkOS	Authentication, identity and session administration; login identifiers, tenant associations and authentication metadata.	Applicable provider infrastructure and support locations; no exclusive regional commitment in this DPA.
Stripe	Payment, invoice and subscription processing; billing contacts, payment references and transaction information. Some activities are performed in Stripe's separate legal role.	Applicable Stripe service and support locations.
Google Workspace	Transactional email; recipient information and message contents appropriate to the notification.	Applicable Workspace service and support locations.
Cloudflare	DNS and configured edge services; relevant hostname, connection and request information.	Global provider network.

Google Analytics and Google Ads measurement are described separately in the Privacy Notice. They do not receive authority under this table to use employer record contents for advertising. Adding a different AI provider requires the applicable provider-change process. Third-party AI hosts that a user connects through a customer-enabled integration are outside this table; the Terms govern them.

Annex D Retention categories

The following categories describe the applicable retention framework. Actual retention must comply with section 9 and the limits in this DPA.

Customer records follow section 9 and the actual employer's lawful recordkeeping instructions. The consultant's loss of access does not erase those records. Ordinary operational logs follow their configured schedule and justified security needs. Google Cloud required administrative and system audit logs remain in the required bucket for 400 days; separately exported copies have separate schedules. Billing, tax, acceptance, dispute and privacy-request evidence is retained for its applicable legal or accountability purpose. AI provider records and caches follow the actual service's lawful and compatible terms and configuration. Backups remain protected until scheduled expiry, with deletion and permission restrictions reapplied on recovery.

SafeGora must document the relevant periods or objective criteria, review continuing needs and make relevant information available for a reasonable compliance request. The documented retention schedule must reflect the applicable provider service and SafeGora's actual configuration, within the limits of this DPA. Any agreed more specific schedule must be compatible with mandatory provider retention and applicable law.

Annex E Contacts and requests

Send privacy, incident, processing-instruction and provider-objection notices to Ollie@safegora.com, identifying the Customer and the affected account or employer without including unnecessary sensitive data. SafeGora will use the Customer's maintained authorized contact for notices. Each party must keep its contact information current. Actual authority must be verified before releasing information or changing another organization's records. The Terms govern ordinary notice timing; urgent incidents and statutory requests remain subject to their applicable duties and deadlines.