

Data Processing Addendum

Vesperion Gate Inc. · Last updated: October 22, 2026 · The current edition is published at <https://www.vesperiongate.com/policies/dpa>

This Data Processing Addendum (“DPA”) forms part of the [Terms of Service](#) between Vesperion Gate Inc. (“Vesperion Gate”) and the customer that owns the applicable service account (“Customer”). It applies when we process personal information in Customer content on Customer's behalf (“Customer Personal Data”). It does not convert our separate billing, account administration, or business operations into processing on Customer's behalf.

“Applicable Data Protection Law” means privacy and data-protection law applicable to that processing, including PIPEDA, the GDPR, the UK GDPR, and applicable US state privacy laws. “Controller,” “processor,” “personal data breach,” and “subprocessor” have their applicable legal meanings. If Customer is itself a processor, it must be authorized by its controller to appoint us as a subprocessor.

This addendum is also available as a [PDF](#) and as [Markdown](#).

1. Scope and instructions

Customer determines the purposes of its processing and warrants that it has the rights, legal basis, and notices or consents needed for its instructions. We will process Customer Personal Data only on documented instructions to provide, secure, support, and terminate the requested Services, unless applicable law requires otherwise. We will inform Customer of a legal requirement before processing unless the law prohibits that notice.

Documented instructions include this agreement, service configuration, authorized use of product features, and supported requests from Customer's users, integrations, or agent members. An integration authorizes only processing within its actual permissions; it does not authorize us to use Customer content for general-purpose model training. If we believe an instruction infringes Applicable Data Protection Law, we will inform Customer and may suspend the affected processing while the parties resolve it.

Annex A describes the subject matter, nature, purposes, duration, data types, and data subjects. Customer-selected external tools are not our subprocessors merely because Customer connects them. We remain responsible for the processing performed by us and providers we engage.

2. Confidentiality, security, and assistance

We will limit access to people who need it for authorized purposes and ensure they are bound by confidentiality duties. We will maintain technical and organizational safeguards appropriate to the

risk, including the measures in Annex B, and will not materially reduce their overall protection during the term.

Taking account of the nature of processing and information available to us, we will assist Customer with data-subject requests, security obligations, breach response, data protection impact assessments, and consultation with supervisory authorities. We will promptly forward a request concerning Customer Personal Data to Customer unless prohibited and will not independently decide its response except as required by law or authorized instructions.

We will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. We will provide available information about its nature, affected data and people, likely consequences, mitigation, and a contact point, with updates as further information becomes available. We will cooperate in investigation and remediation. Customer remains responsible for notices it must give to regulators and affected people; our notice does not delay its legal deadlines.

3. Subprocessors

Customer acknowledges and agrees that we may engage subprocessors to provide the Services. We have a written agreement with each subprocessor containing data protection obligations not less protective than those in this DPA, to the extent applicable to the nature of the services it provides, including confidentiality, security, deletion, assistance, and applicable international-transfer safeguards. We remain responsible for its performance of those obligations. We will not authorize a provider to train general-purpose AI models using private Customer content.

We make the current list of subprocessors available in the [provider register](#) and record changes in the [policy update history](#). We will post notice of a new or replacement subprocessor before authorizing it to process Customer Personal Data. Customers who want to be notified of subprocessor changes must subscribe to our [policy updates](#), by email or feed.

Customer may object to a new subprocessor by notifying privacy@vesperiongate.com in writing within ten (10) business days after we post that notice. On receiving an objection we may, at our choice, look for a reasonable change to the Services, or suggest a commercially reasonable change to how Customer has configured or uses them, so that the new subprocessor never processes Customer Personal Data and Customer is not unreasonably burdened. If we cannot make such a change available within a reasonable period, not to exceed thirty (30) days, Customer may terminate, with written notice, the affected Services that cannot be provided without the new subprocessor. As of the effective date of that termination, we will refund any prepaid fees for the terminated Services covering the remainder of the term and will not penalize Customer for the termination.

4. Return, deletion, and retention

Customer can export available content while its account remains accessible or request assistance before closure. At the end of processing, we will delete or return Customer Personal Data as instructed and delete existing copies unless applicable law requires retention. Product recovery periods, scheduled removal, and restricted backup rotation are described in the [Privacy Policy](#) and Annex A. Contact us if a specific lawful erasure instruction requires a different process.

Retained copies remain protected and cannot be used for another purpose. If a backup is restored, applicable deletion instructions must be reapplied before the content returns to ordinary use. Separate records that we lawfully need for security, accounting, or legal compliance are limited to those purposes and their applicable schedules.

5. Demonstrating compliance and audits

We will make available information necessary to demonstrate compliance with this DPA and allow and contribute to audits, including inspections, by Customer or an independent auditor it appoints. The parties will first use relevant documentation and reasonable questionnaires where sufficient. An inspection may be necessary where that information is insufficient, a material concern exists, or law or a regulator requires it.

The parties will coordinate reasonable notice, scope, confidentiality, and measures to protect other customers and service security. These arrangements must not prevent a legally required audit or delay urgent regulatory access. Any exceptional assistance charges must be agreed in advance and must not defeat mandatory rights.

6. California and similar US state requirements

Where we act as a service provider or contractor under applicable US state privacy law, we will not sell or share Customer Personal Data, retain, use, or disclose it outside the specified business purposes and direct business relationship, or combine it with other personal information except where the law permits. We will comply with applicable obligations and provide the legally required level of privacy protection.

Customer may take reasonable steps to verify that use is consistent with its obligations and to stop and remediate unauthorized use. We will notify Customer if we determine that we can no longer meet those obligations. We certify that we understand and will comply with these restrictions.

7. International transfers

Customer instructs processing in the locations disclosed in the Privacy Policy and provider register, subject to safeguards required by Applicable Data Protection Law. We must establish an applicable lawful transfer mechanism for a restricted transfer, including relevant onward transfers. We will provide reasonably requested information for Customer's transfer assessment and cooperate with supplementary safeguards where required.

Where a transfer to Vesperion Gate requires EU Standard Contractual Clauses and no applicable adequacy decision or other valid mechanism covers it, the clauses in the Annex to [Commission Implementing Decision \(EU\) 2021/914](#) ("SCCs") are incorporated without modification: Module Two applies to controller-to-processor transfers and Module Three to processor-to-processor transfers. Clause 7 applies; Clause 9 uses Option 2 with at least ten (10) business days' prior notice; the optional text in Clause 11 does not apply; Clause 17 selects Irish law and Clause 18 selects the courts of Ireland. The competent supervisory authority is determined under Clause 13. Annexes A and B below complete SCC Annexes I and II; the register identifies authorized subprocessors.

For UK restricted transfers requiring these safeguards, the [ICO International Data Transfer Addendum, version B1.0](#), including its mandatory clauses as revised under Section 18, is incorporated. Table 1 uses the parties, contacts, and effective date in Annex A; Table 2 uses the SCCs and selections above; Table 3 uses Annexes A and B; and Table 4 permits either party to end the Addendum as allowed by Section 19. Its mandatory clauses prevail for UK transfers.

For Swiss transfers relying on the SCCs, references to the GDPR include the applicable Swiss Federal Act on Data Protection, the competent authority is the Swiss Federal Data Protection and Information Commissioner where applicable, and references to a Member State include Switzerland to the extent required to preserve Swiss data subjects' rights. These adaptations do not remove protections for EEA data subjects.

The parties must complete any missing customer identity, address, contact, or transfer details required by the SCCs before relying on them. Contact privacy@vesperiongate.com for a completed copy or a different required transfer arrangement. Publication of this DPA does not certify a provider's eligibility under an adequacy framework or establish contracts with that provider.

8. Priority and duration

This DPA continues while we process Customer Personal Data, including restricted retained copies. It prevails over conflicting general Terms on data protection; mandatory SCC or UK Addendum provisions prevail over both. Nothing limits a data subject's rights, mandatory liability, or a regulator's powers. A separately executed DPA applies where it expressly replaces this one.

Annex A: Processing and parties

- **Customer / exporter:** the account-owning legal entity or individual identified in the service agreement and account or billing records, at the address recorded there. Contact: its designated account owner or privacy contact. Role: controller, or processor acting under its controller's authorization.
- **Vesperion Gate / importer:** Vesperion Gate Inc., 901 Guelph Line, Burlington, Ontario L7R 3N8, Canada. Contact: privacy@vesperiongate.com. Role: processor or subprocessor. Activities: providing the contracted Services.
- **Agreement and date:** acceptance of the applicable Terms or a signed service agreement binds the parties to this DPA. Transfer clauses apply from the first transfer for which they are required, subject to completion of required party details.
- **Data subjects:** Customer's users, employees, contractors, clients, collaborators, contacts, and other people whose information Customer includes. LensCherry inputs may depict consenting adults.
- **Data types:** identity and contact information; organization and project details; tasks, messages, documents, files, comments, chat, schedules and activity; prompts, photos, reference profiles and generated content; and technical identifiers and metadata needed to provide and secure the relevant feature.
- **Sensitive data:** the Services are not designed for regulated clinical records, payment-card storage, government identifiers, or authentication secrets in customer content. Customer must not use MCP tool content for those categories. Other sensitive information must be limited to what is lawful and necessary, with suitable access restrictions and a provider arrangement appropriate to it. Free-text content is not represented as automatically screened.
- **Nature, purpose, and frequency:** ongoing collection, organization, storage, retrieval, transmission, display, authorized modification, support, security, and deletion. LensCherry includes customer-requested generation and safety screening. Customer-selected integrations receive information at Customer's direction and within supported permissions.
- **Duration:** the account term followed by the applicable recovery, deletion, backup, and limited-record retention schedules in the Privacy Policy. Provider-specific processing periods appear in the register.

Annex B: Security measures

- HTTPS for public product connections; encryption at rest for stored files and encrypted database backups. Application data is not end-to-end encrypted.
- Authenticated access, account and project authorization, credential revocation, and restricted administrative access. Thicket supplements application checks with PostgreSQL row-level security.
- Separation of production and development storage, restricted backup credentials, firewalls, network protection, and operational monitoring.
- Daily backups, offsite file replicas, documented recovery procedures, scheduled retention cleanup, and reapplication of deletion instructions after recovery.
- Security and diagnostic records, incident response, dependency maintenance, and verification of changes before deployment.
- Confidentiality duties, purpose-limited staff access, data minimization, and provider review before new customer-data processing.

Product-specific measures are described on the [Trust and Security page](#). These measures do not constitute a claim of an independent certification or a guarantee that incidents cannot occur.