Data Processing Agreement

Wizer Email Security

Effective when accepted alongside the Wizer Email Security Subscription Agreement.

v0 draft — pending review by legal counsel. Customers requiring a counter-signed DPA should request the executable version from `legal@wizer-training.com` *.*

---

1. Parties

This Data Processing Agreement ("**DPA**") forms part of the Wizer Email Security Subscription Agreement (the "**Agreement**") between **Wizer Training, Inc.**, a Delaware corporation with offices at 131 Dartmouth St, Boston, MA 02116, USA ("**Wizer**", "**we**", "**Processor**") and the customer identified in the Order Form ("**Customer**", "**Controller**").

Where Customer is itself acting as a processor on behalf of its own end customers (e.g., an MSP), Customer represents that it has authority to bind those end customers to terms substantively equivalent to this DPA.

2. Definitions

Terms not defined here have the meanings given in the Agreement. The terms "**personal data**", "**processing**", "**controller**", "**processor**", "**data subject**", "**data protection laws**", and "**supervisory authority**" have the meanings given in applicable data protection laws, including the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK GDPR, and the California Consumer Privacy Act as amended by the CPRA ("**CCPA/CPRA**").

"**Customer Data**" means personal data processed by Wizer on behalf of Customer in connection with the Service.

"**Service**" means the Wizer Email Security software-as-a-service product as described in the Agreement.

"**Sub-processor**" means any third party engaged by Wizer to process Customer Data on Wizer's behalf.

3. Scope and Roles

Customer is the **controller** of Customer Data. Wizer is the **processor** acting on Customer's documented instructions.

Wizer will not process Customer Data for any purpose other than performing the Service under the Agreement and complying with applicable law.

4. Duration

This DPA takes effect on the same date as the Agreement and remains in force for the term of the Agreement plus any period during which Wizer retains Customer Data.

5. Subject Matter, Nature, and Purpose of Processing

The subject matter, nature, purpose, categories of data subjects, and categories of personal data are described in **Annex I**.

6. Processor Obligations

Wizer will:

- (a) process Customer Data only on documented instructions from Customer, including the Agreement, this DPA, and the Service configuration set by Customer's administrators;
- (b) ensure that personnel authorized to process Customer Data are bound by confidentiality obligations;
- (c) implement and maintain appropriate technical and organizational measures to protect Customer Data, as described in **Annex II**;
- (d) only engage Sub-processors in accordance with Section 8 and **Annex III**;
- (e) assist Customer in responding to data subject requests, in carrying out data protection impact assessments, and in consulting with supervisory authorities;
- (f) notify Customer of any personal data breach affecting Customer Data without undue delay and no later than seventy-two (72) hours after becoming aware;
- (g) make available to Customer the information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits as described in Section 11; and
- (h) at Customer's choice, return or delete Customer Data at the end of the Service in accordance with Section 12.

7. Confidentiality

Wizer's staff with access to Customer Data are bound by written confidentiality obligations. By design, Wizer's central control plane does not provide Wizer staff with read access to per-row tenant data (see Annex II § "Architectural Isolation").

8. Sub-processors

Customer grants Wizer general authorization to engage Sub-processors, subject to this Section.

Wizer maintains a current list of Sub-processors at **Annex III**. Wizer will notify Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days in advance. Customer may object on reasonable data-protection grounds; if the parties cannot resolve the objection, Customer may terminate the affected portion of the Service.

Wizer remains liable to Customer for the acts and omissions of its Sub-processors with respect to Customer Data.

9. Data Subject Rights

Wizer will provide Customer with the technical means to access, correct, export, or delete Customer Data through the administrator console. Where Customer cannot accomplish a data subject request through self-service, Wizer will assist Customer at no additional cost (where assistance is required of a processor by applicable law).

10. Security Incidents

Wizer will:

- (a) notify Customer in writing without undue delay (and within seventy-two (72) hours of confirmation) of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data;
- (b) provide the information Customer needs to satisfy any obligation to notify a supervisory authority and/or data subjects; and

- (c) take reasonable steps to mitigate the effects of the breach.

Routine unsuccessful access attempts (e.g., normal port-scan noise, blocked credential-stuffing attempts) do not constitute a security incident under this Section.

11. Audits

Customer (or an independent third-party auditor reasonably acceptable to Wizer and bound by confidentiality obligations) may audit Wizer's compliance with this DPA, no more than once per twelve (12) month period and on reasonable prior written notice, during normal business hours and in a manner that does not unreasonably interfere with Wizer's operations.

In place of an on-site audit, Wizer may provide Customer with then-current independent third-party attestations (e.g., SOC 2 Type 1 / Type 2 reports once issued) and respond to a customer security questionnaire.

12. Return or Deletion

At Customer's written request following termination of the Agreement, Wizer will either return or permanently delete Customer Data within thirty (30) days, except where retention is required by applicable law. Wizer will provide written confirmation of deletion on request.

13. International Data Transfers

To the extent Wizer processes Customer Data originating from the European Economic Area, the United Kingdom, or Switzerland in a country that has not been deemed to provide an adequate level of protection, the parties agree that the European Commission's Standard Contractual Clauses (Module 2 — controller to processor), the UK International Data Transfer Addendum, or equivalent transfer mechanism, are hereby incorporated by reference and signed by acceptance of this DPA. Customer is the "data exporter" and Wizer is the "data importer".

14. CCPA / CPRA

To the extent Wizer processes personal information subject to the CCPA/CPRA, Wizer is acting as a "service provider" as defined in the CCPA/CPRA. Wizer:

- (a) will not sell or share Customer Data;
- (b) will not retain, use, or disclose Customer Data outside of the direct business relationship between Wizer and Customer or for any purpose other than the specific business purpose of providing the Service;
- (c) will not combine Customer Data received from Customer with personal information received from any other source except as permitted by CCPA/CPRA for service providers; and
- (d) certifies that it understands these restrictions.

15. Liability

Each party's liability under or in connection with this DPA is subject to the limitation of liability provisions in the Agreement.

16. Conflict

In the event of any conflict between this DPA and the Agreement, this DPA controls with respect to the processing of Customer Data. Otherwise, the Agreement controls.

17. Changes

Wizer may update this DPA from time to time to reflect changes in law, sub-processors, or the Service. Material changes will be notified to Customer at least thirty (30) days in advance.

Annex I — Description of Processing

Subject matter: Detection and triage of phishing, business-email-compromise (BEC), and related email-borne threats targeting Customer mailboxes.

Duration: For the term of the Agreement and any wind-down period defined in Section 12.

Nature and purpose: Automated detection rules and AI-assisted second-opinion analysis applied to inbound email metadata; presentation of warning banners, quarantine routing, and reporting affordances to mailbox users; administrative console for Customer's IT/security staff.

Categories of personal data processed:

- Email message metadata: sender address, sender display name, recipient mailbox, subject line, routing and authentication headers, hyperlinks, and attachment metadata (filename, MIME type, size).
- Detection records: rule firings, AI second-opinion verdicts, banner actions taken by users.
- Administrator account information: name, email address, profile image URL (received from Google sign-in only).

Categories NOT processed:

- Message body content beyond the parsed enrichment signals.
- Attachment contents.
- Any data unrelated to detection.

Categories of data subjects: Customer's employees and contractors whose mailboxes are enrolled in the Service; senders of inbound mail to those mailboxes (as data subjects of message metadata).

Geographic scope: Customer Data is stored within the United States. Specific regional placement is available on request for customers subject to regional data-residency requirements.

Annex II — Technical and Organizational Measures

Architectural Isolation

- **Per-tenant database**. Each Customer is provisioned with a dedicated Postgres database. No row of Customer Data shares a database with another Customer.
- **Per-tenant deployment**. Each Customer's application instance is a separate serverless deployment with isolated credentials and a separate inbound Pub/Sub subscription.

- **No-cross-tenant rule sharing**. Detection rules synthesized from one Customer's reports are never propagated to another Customer without explicit opt-in.
- **Central control-plane isolation**. Wizer's central management surface is the source of truth for license + billing + tenant lifecycle, and by design has no access to per-row Customer Data. Wizer staff cannot read Customer message metadata except where Customer grants explicit support access.

Encryption

- **In transit:** TLS 1.2 or higher for all connections to and from the Service, including connections to Sub-processors.
- **At rest:** Database storage encrypted at the provider level; application blob storage (used for retained .eml triage attachments, see "Retention" below) encrypted at the provider level.

Access Control

- Administrator access to the tenant console is gated by Google Domain-Wide-Delegation and per-tenant administrator allow-lists.
- Internal access to production systems by Wizer staff is least-privilege, logged, and limited to named operators.

Sub-processor Governance with AI Providers

- **All AI usage** — both inline detection second-opinion and the optional admin agent — runs against Anthropic models routed through the Vercel AI Gateway under a Zero-Data-Retention contract. Prompts and responses are not stored or used for model training.
- Wizer applies a structural anonymization layer before any per-message data reaches an AI provider: real domains and addresses are replaced with placeholders; raw message bodies are not transmitted.
- The optional admin agent may invoke a `web_search` tool routed through a separate third-party search provider. The ZDR contract is with Anthropic specifically and does not extend to that provider. Search queries are derived from the same anonymized inputs, so no tenant-identifying data leaves through that path.

Audit Logging

- All administrator actions in the tenant console are recorded with operator identity, timestamp, and (where applicable) the reason provided.
- The audit log is retained for seven (7) years to support compliance review.

Backup and Recovery

- Each tenant database has seven (7) days of point-in-time recovery enabled.
- Production database branches are protected from accidental deletion.
- Recovery procedure documented and tested; verified restore time under five (5) minutes for the reference deployment as of June 13, 2026.

Retention

- Detection records and audit logs: retained for the term of the Agreement.
- Raw .eml attachments captured for triage: retained for thirty (30) days OR until administrator disposition (whichever is sooner).
- Per-mailbox spam-filter state: retained for the duration the mailbox is monitored.

Vulnerability Management

- Application dependencies monitored continuously; security patches applied through routine release process.
- Code changes subject to automated security review prior to deployment to production.

Personnel

- Wizer staff sign confidentiality agreements as a condition of employment.
- Production access reviewed at least quarterly.

Annex III — Sub-processors

Current as of the Effective Date. Updates published at `https://wizer-emailsecurity.com/privacy#subprocessors` and notified per Section 8.

A sub-processor is a third party engaged by Wizer that processes Customer personal data. Listed by function.

Infrastructure

Sub-processor	Purpose	Location
Vercel, Inc.	Application hosting; AI Gateway routing; encrypted file storage. Email content and metadata pass through and rest here (encrypted at rest).	United States
Neon, Inc.	Per-tenant database hosting. Email metadata, encrypted message bodies, mailbox addresses.	United States

Product functionality

Sub-processor	Purpose	Location
Google LLC	Google Workspace API access to monitored mail (via tenant-granted Domain-Wide Delegation) and Google Cloud Pub/Sub for inbound delivery. Mail metadata and content of monitored mailboxes.	United States

Customer management and support

Sub-processor	Purpose	Location
HubSpot, Inc.	Customer support, success, CRM, and sales operations.	United States
Twilio Inc. (SendGrid)	Transactional and customer-communication emails.	United States
Stripe, LLC	Payment processing and billing.	United States

Not sub-processors (no personal data). The following services support the Service but never receive Customer personal data, so they are not sub-processors: **Anthropic PBC** (all AI usage — inline detection and the optional admin agent — receiving only structurally anonymized inputs under a Zero-Data-Retention contract; message bodies are not transmitted); the **third-party web search** the optional admin agent may invoke (anonymized queries only); **Google Safe Browsing** (URL reputation; URLs only, no message content); and **GitLab, Inc.** (source-code management; no Customer Data). See Annex II § "Sub-processor Governance with AI Providers".

Annex IV — Signature

This DPA is incorporated by reference into the Agreement and is binding on the parties as of the Effective Date of the Agreement without requiring further signature. Customer accepts this DPA by executing the Agreement or by clicking through this DPA in the administrator console (as applicable).

A counter-signed copy may be executed on request to `legal@wizer-training.com`.

Wizer Training, Inc. · 131 Dartmouth St, Boston, MA 02116, USA · `legal@wizer-training.com` · `wizer-emailsecurity.com`