Data Processing Agreement

Version 1.0 · Last updated July 15, 2026

> This Data Processing Agreement is provided for review and is subject to review and finalization by legal counsel before enterprise execution. Contact privacy@mrktmesh.com to execute a signed copy.

1. Parties & Roles

This Data Processing Agreement ("DPA") forms part of the agreement between the merchant using MRKT Mesh (the "Merchant," acting as **data controller**) and **Language Commerce Inc** ("Mesh," acting as **data processor**), and governs Mesh's processing of personal data of the Merchant's customers ("Customer Personal Data") on the Merchant's behalf.

"Data Protection Laws" means the laws applicable to the processing of Customer Personal Data under this DPA, including the EU and UK GDPR and the CCPA/CPRA where applicable. [COUNSEL: definitions to align with the executed master terms.]

2. Subject Matter, Duration, Nature & Purpose

- **Subject matter:** server-side conversion measurement for the Merchant's store and, at the Merchant's direction, delivery of conversion events to marketing destinations the Merchant configures.
- **Duration:** the term of the Merchant's use of the service, plus the deletion periods in Section 9.
- **Nature and purpose:** collection of commerce events from the Merchant's store platform and storefront, pseudonymization/hashing of identifiers at ingestion, attribution measurement, accuracy monitoring, and Merchant-directed transmission to destinations.

3. Categories of Data Subjects & Personal Data

Data subjects: customers and visitors of the Merchant's store.

Categories of Customer Personal Data (detailed in Annex A): SHA-256-hashed email and phone; the store's numeric customer identifier; a first-party visitor identifier; advertising click identifiers and cookies (fbclid/gclid/ttclid, fbp/fbc); IP address and user agent; order and cart details (order ID, items, totals, currency); attribution data (UTM parameters, landing page, referrer); and recorded consent state.

Excluded by design: raw email, raw phone, names, postal addresses, and payment details are not retained — they are hashed or removed by a default-deny sanitization boundary before storage. No special categories of data are processed.

4. Processor Obligations

Mesh will:

- process Customer Personal Data only on the Merchant's documented instructions — given through the service's configuration surfaces (installation, destination connections, forwarding controls) — unless required otherwise by law, in which case Mesh informs the Merchant unless legally prohibited;
- ensure persons authorized to process the data are bound by confidentiality;
- implement the technical and organizational measures in Annex B;
- respect the subprocessor conditions in Section 6 and assist the Merchant per Sections 7 and 8;
- delete Customer Personal Data as described in Section 9;
- make available information reasonably necessary to demonstrate compliance, per Section 10;
- not sell Customer Personal Data, not retain, use, or disclose it for any purpose other than providing the service, and not combine it with data from other merchants (CCPA/CPRA service provider commitments).

5. Security Measures

Mesh implements the measures described in Annex B, including: encryption of credentials and store tokens at rest (AES-256-GCM); SHA-256 hashing of email/phone at ingestion with raw values never persisted; a default-deny ingestion boundary that

rebuilds payloads from an allowlist; TLS for data in transit; HMAC authentication of inbound store webhooks; role-based access control; an append-only audit log of configuration changes; and service-level secrets provisioned through a managed secret manager.

6. Subprocessors

- The Merchant provides general authorization for the subprocessors listed at /subprocessors (currently Google Cloud Platform for hosting and data processing, and Resend for operational email).
- Mesh will update that page before engaging a new subprocessor and provide a mechanism for notice; the Merchant may object on reasonable data-protection grounds, in which case the parties will work in good faith toward a resolution, including the Merchant's right to terminate the affected service.
- Mesh remains responsible for its subprocessors' performance and imposes data-protection obligations consistent with this DPA on them.
- **Destinations are not subprocessors.** Marketing platforms the Merchant connects (Meta, Google Analytics 4, TikTok, Klaviyo) are third-party recipients to which the Merchant directs disclosure; they process data under their own terms and the Merchant's relationship with them.

7. Assistance with Data-Subject Rights

Taking into account the nature of processing, Mesh assists the Merchant in responding to data-subject requests, in the first instance through automation already built into the service:

- **Erasure:** on the store platform's customer erasure webhook, Mesh deletes the customer's session records and removes identity data from the customer's event records; de-identified commerce records remain.
- **Access:** on the platform's data-request webhook, Mesh acknowledges the request and fulfills it through its support process with the Merchant.
- Requests reaching Mesh directly from data subjects are referred to the Merchant without undue delay.

8. Personal Data Breach Notification

Mesh will notify the Merchant without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and will provide information reasonably available to help the Merchant meet its own notification obligations. [COUNSEL: fixed notification window (e.g., 48/72 hours) and notice channel.]

9. Deletion & Return of Data

- **Automatic:** event, delivery, and session records are deleted by a scheduled job after 90 days; on uninstall, the store platform's erasure webhook triggers deletion of the store's events, sessions, delivery records, and registration.
- **On request:** remaining Customer Personal Data (including analytics warehouse records, which carry only hashed or pseudonymous identity) is deleted on the Merchant's written request within a commercially reasonable period, unless retention is required by law.

10. Audits & Information

Mesh will make available information reasonably necessary to demonstrate compliance with this DPA (including this document, the subprocessor list, and summaries of the measures in Annex B) and will allow for and contribute to audits conducted by the Merchant or its mandated auditor, subject to reasonable notice, frequency, confidentiality, and scope limits. [COUNSEL: audit cost allocation.]

11. International Transfers

Customer Personal Data is processed in the United States. For transfers of EU/EEA or UK personal data, the parties rely on Standard Contractual Clauses, which are incorporated into this DPA by reference. [COUNSEL: select SCC modules (expected: Module 2, controller-to-processor), UK addendum, and complete the required annex designations before execution.]

12. Liability

Each party's liability under this DPA is subject to the limitations of liability in the parties' agreement. [COUNSEL: confirm interaction of DPA liability with the master terms cap.]

13. Governing Law

[COUNSEL: governing law of this DPA, aligned with the master terms.]

Annex A — Processing Details

- **Data subjects:** the Merchant's store customers and storefront visitors.
- **Personal data:** hashed contact identifiers (SHA-256 email/phone); store customer ID; first-party visitor ID; advertising click IDs and cookies; IP address; user agent; order/cart contents and amounts; attribution parameters; consent state.
- **Sensitive data:** none processed.
- **Frequency:** continuous, event-driven.
- **Processing operations:** ingestion with sanitization/hashing, storage, attribution measurement, accuracy monitoring, Merchant-directed delivery to destinations, deletion.

Annex B — Technical & Organizational Measures

- **Minimization at ingestion:** default-deny payload rebuild from field allowlists; names, addresses, and payment details removed; email/phone replaced by SHA-256 hashes; free text screened for stray identifiers.
- **Encryption:** AES-256-GCM for merchant credentials and store tokens at rest; TLS in transit; service-level secrets in a managed secret manager.
- **Authentication & access:** HMAC-verified inbound webhooks; bcrypt-hashed dashboard passwords or Google SSO; role-based access control on sensitive operations.
- **Accountability:** append-only audit log of configuration changes (no credential values, boolean metadata only).
- **Egress control:** events leave only to Merchant-configured destinations; identifiers sent to destinations are hashed or pseudonymous per the Privacy Policy; raw email/phone, names, and addresses are never transmitted.
- **Retention:** scheduled 90-day deletion of event, delivery, and session records; automated queue pruning; webhook-driven erasure (Annex A operations, Section 9).
- **Infrastructure:** Google Cloud Platform (us-east1), single-region service footprint; logical tenant separation per store.

Annex C — Subprocessors

The authorized subprocessor list is maintained at /subprocessors and forms part of this DPA.

Contact

privacy@mrktmesh.com
Language Commerce Inc