DATA PROCESSING AGREEMENT

Effective Date: _____

This Data Processing Agreement ("**DPA**") is entered into between:

Mesh Intelligent Technologies, Inc. (d/b/a Pieces.app) ("**Processor**" or "**Provider**")

and

_____ ("**Controller**" or "**Customer**")

This DPA supplements and forms part of the Master Service Agreement between the parties dated _____ (the "**Agreement**" or "**MSA**").

---

1. DEFINITIONS

1.1 Terms used in this DPA have the meanings given in the MSA unless otherwise defined herein.

1.2 The following terms have the meanings given by the EU General Data Protection Regulation ("**GDPR**") and shall apply equally to similar concepts in other privacy laws:

- "**Personal Data**" means any information relating to an identified or identifiable natural person
- "**Data Subject**" means the natural person to whom Personal Data relates
- "**Processing**" means any operation performed on Personal Data
- "**Controller**" means the entity that determines the purposes and means of Processing
- "**Processor**" means the entity that Processes Personal Data on behalf of the Controller
- "**Sub-processor**" means any processor engaged by the Processor
- "**Supervisory Authority**" means an independent public authority with data protection oversight

1.3 "**Data Protection Laws**" means all applicable laws relating to privacy and data protection, including:

- EU/UK General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA) and CPRA
- Other US state privacy laws (Virginia, Colorado, etc.)
- Australian Privacy Act and APP

- Canadian PIPEDA
- Any other applicable privacy regulations

In the event of a conflict between applicable Data Protection Laws, the parties shall confer in good faith to determine the appropriate course of action, prioritizing the most protective standard for Data Subjects.

---

2. PROCESSING OF PERSONAL DATA

2.1 Architecture & Data Residency. The parties acknowledge that Pieces operates with a **primarily on-device architecture**:

Data Persistence:

- **On-Device Storage (>99% of all persistent data):**
    - ALL code snippets, files, and development content
    - ALL AI conversation history and context
    - ALL personal workflow data and history
    - ALL sensitive intellectual property
    - ALL processing results and outputs
    - Local LLM/SLM models and embeddings
- **Cloud Metadata Only (<1% - minimal operational data):**
    - Authentication tokens (SSO/login state)
    - Crash analytics metadata (PII scrubbed)
    - Anonymized/abstract usage metrics (opt-in)
    - License validation keys
    - Abuse detection signals

Processing Architecture:

- **On-Device Processing (~85% in blended mode):**
    - All data ingestion and storage
    - Local model inference
    - Data organization and retrieval
- **Ephemeral Cloud Processing (~15% in blended mode):**
    - Input/output operation for LLM inference ONLY

    - Zero persistence of inputs or outputs
    - Pure computational service - no data retention
    - Results immediately transferred to device for local storage
    - Provider does not store processing data unless explicitly requested by Customer for auditing. Any storage of processing data for auditing purposes shall be subject to the same security, access, and deletion protocols as other Personal Data under this DPA

- Cloud proxy services handle gRPC-to-REST translation, authentication, and policy enforcement (required even for BYOK)

Configuration Options:

- **Blended Mode (Default):** ~85% on-device, ~15% cloud processing for enhanced AI
- **Air-Gapped Mode:** 100% on-device with local SLMs (reduced capabilities)
- **Enterprise Controls:** Org-wide LLM restrictions, SSO-locked models, or BYOK options (all requiring cloud proxy services)

Critical Note: This DPA governs minimal cloud metadata AND ephemeral cloud processing operations. In Air-Gapped Mode, the product operates entirely offline without any cloud connectivity. Customer acknowledges that BYOK data will transit Provider's cloud infrastructure even when using Customer's own LLM API keys. Provider will notify Customer in writing at least 30 days in advance of any changes to the technical architecture that may affect data residency or security. If Customer's regulatory requirements change and cannot be met due to this limitation, Customer may terminate the affected SOW with a pro-rated refund.

2.2 Relationship of the Parties. The parties acknowledge that with regard to Processing of Personal Data:

- Customer is the Controller (or where Customer acts on behalf of another Controller, Customer is a Processor)
- Provider is a Processor acting on Customer's behalf
- This DPA applies only when Provider Processes Personal Data in cloud services

2.3 Customer Instructions. Provider shall:

- Process Personal Data only on documented instructions from Customer
- Use cloud processing for AI features only as configured by Customer (blended, SSO-locked, BYOK, or disabled)
- Cloud proxy services are required for all LLM operations (including BYOK) to handle secure protocol translation, authentication, and policy enforcement
- Immediately inform Customer if an instruction infringes Data Protection Laws (in Provider's opinion)
- Not Process Personal Data for any purpose other than providing the Services

- Not retain Personal Data from ephemeral cloud processing after completion
- Provider acknowledges it has no technical capability to remotely access locally-stored on-device data

2.4 Data Processing Details. The details of Processing are described in **Appendix 1**.

2.5 Duration. Processing shall continue for the duration of the Agreement unless otherwise agreed.

---

3. PROCESSOR OBLIGATIONS

3.1 Compliance. Provider shall comply with all applicable Data Protection Laws in Processing Personal Data.

3.2 Confidentiality. Provider shall:

- Ensure all personnel authorized to Process Personal Data are bound by confidentiality
- Maintain the confidentiality of all Personal Data
- Not disclose Personal Data to third parties except as permitted herein

3.3 Security of Processing. Provider shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Encryption of Personal Data in transit and at rest
- Ongoing confidentiality, integrity, availability, and resilience of systems
- Ability to restore availability and access to Personal Data timely
- Regular testing, assessment, and evaluation of security measures
- Measures listed in **Appendix 2**

Provider shall promptly notify Customer of any material changes to the technical and organizational measures described in Appendix 2.

3.4 Data Subject Rights. Provider shall:

- Assist Customer in responding to Data Subject requests
- Implement appropriate measures to facilitate Customer's obligations
- Notify Customer promptly of any Data Subject request received directly
- Not respond to Data Subject requests except on Customer's documented instructions

3.5 Data Protection Impact Assessment. Provider shall provide reasonable assistance for Customer's:

- Data protection impact assessments
- Prior consultations with Supervisory Authorities
- Other compliance obligations under Data Protection Laws

3.6 Personnel. Provider shall:

- Limit access to Personal Data to personnel who need to know
- Ensure personnel are subject to appropriate confidentiality obligations
- Provide appropriate training on data protection
- Take appropriate action against personnel who violate this DPA

---

4. SUB-PROCESSORS

4.1 Authorized Sub-processors. Customer provides general authorization for Provider to engage Sub-processors listed in **Appendix 3**.

4.2 Requirements for Engagement. Provider shall:

- Enter into written agreements with Sub-processors imposing data protection obligations no less protective than this DPA
- Remain fully liable for Sub-processor performance
- Ensure Sub-processors comply with Data Protection Laws

4.3 Changes to Sub-processors. Provider shall:

- Maintain a current list of Sub-processors at [https://pieces.app/legal/subprocessors]
- Notify Customer of intended additions or replacements at least 30 days in advance
- Provide opportunity for Customer to object to changes
- Customer shall have the right to reasonably object to the appointment of a new Sub-processor within 30 days of notice. 'Reasonable grounds' shall include, but not be limited to, concerns regarding the Sub-processor's data protection practices, location, or regulatory compliance. If Customer objects, Provider shall work in good faith to address the objection, and if not resolved, Customer may terminate the affected services without penalty
- Offer termination rights if Customer reasonably objects and Provider cannot accommodate

---

5. INTERNATIONAL TRANSFERS

5.1 Transfer Mechanisms. For transfers of Personal Data outside the EEA/UK/adequate countries:

- Provider shall ensure appropriate safeguards per Data Protection Laws
- The parties shall execute Standard Contractual Clauses ("**SCCs**") as required
- Provider may rely on other valid transfer mechanisms (adequacy decisions, certifications)

5.2 Standard Contractual Clauses. Where required:

- The SCCs are incorporated by reference. For the avoidance of doubt, the Standard Contractual Clauses incorporated herein refer to the most recent version adopted by the European Commission as of the Effective Date of this DPA, unless otherwise agreed in writing
- Customer is the "data exporter" and Provider is the "data importer"
- The optional clauses in **Appendix 4** shall apply

5.3 Supplementary Measures. Provider implements supplementary measures including:

- Technical measures (encryption, pseudonymization)
- Organizational measures (access controls, training)
- Contractual measures (enhanced commitments)

---

6. SECURITY BREACHES

6.1 Notification. Provider shall notify Customer without undue delay (and within 24 hours) after confirming a Personal Data breach that affects Customer's Personal Data, including:

- Nature of the breach
- Categories and approximate number of Data Subjects affected
- Categories and approximate number of Personal Data records affected
- Likely consequences
- Measures taken or proposed to address the breach

Provider shall provide regular updates to Customer regarding the status of breach investigation and remediation until resolution.

6.2 Cooperation. Provider shall:

- Cooperate with Customer in investigating and remediating breaches

- Document all breaches and remediation efforts
- Not publicly disclose breaches without Customer's prior written consent (except as legally required)

6.3 Mitigation. Provider shall take immediate steps to mitigate effects and prevent recurrence.

---

7. AUDIT AND INSPECTION

7.1 Audit Rights. Provider shall make available all information necessary to demonstrate compliance with this DPA and allow for audits, including inspections. Provider conducts quarterly internal security reviews with evidence available upon request.

7.2 Audit Process:

- Customer may exercise audit rights annually with 30 days' written notice
- Audits shall be conducted during business hours through document review, questionnaires, and evidence provision (not direct system access)
- Customer shall bear its own audit costs (unless material non-compliance is found)
- Provider may require execution of confidentiality agreements
- Most audit requirements can be satisfied through Provider's SOC 2 Type II reports and other compliance certifications
- In the event of a material security incident or regulatory investigation, Customer may request expanded audit rights, subject to reasonable confidentiality and security controls

7.3 Certifications. Provider shall maintain and provide upon request:

- SOC 2 Type II reports (or equivalent)
- ISO 27001 certification (if applicable)
- Other relevant compliance certifications

---

8. DATA RETENTION AND DELETION

8.1 Retention. Provider shall:

- Not retain Personal Data longer than necessary for Processing purposes
- Delete or return Personal Data upon Customer's request
- Delete existing copies unless retention is required by law

8.2 Data Export & Deletion Process.

Export for On-Device Software:

- Personal Data primarily resides on Customer's end-user devices (macOS, Windows, Linux)
- Provider offers export tools and documentation on a best-effort basis:
    - Local database export utilities provided within the application
    - API access for programmatic data extraction where available
    - Technical support for data migration questions
- Customer acknowledges that data format and structure may vary based on application version
- Provider is not responsible for data already stored locally on end-user devices

Deletion Timeline:

- Customer has 60 days post-termination to export cloud-stored data
- Provider shall delete cloud-hosted Personal Data within 30 days (standard) or 60 days (complex)
- Backup deletion within 35 days of primary deletion
- Deletion certification provided upon request. Provider shall provide written confirmation of deletion within 30 business days of completion, upon Customer's request
- Note: Data on end-user devices must be deleted by Customer/end-users

8.3 Legal Retention. If law requires retention, Provider shall:

- Inform Customer of the legal requirement (unless prohibited)
- Protect the Personal Data from further Processing
- Delete the Personal Data once retention period expires

---

9. CONTROLLER OBLIGATIONS

9.1 Lawful Basis. Customer warrants that:

- It has and will maintain valid legal basis for Processing
- It has provided necessary notices to Data Subjects
- It has obtained necessary consents where required

9.2 Instructions. Customer shall:

- Provide clear, lawful instructions for Processing
- Ensure instructions comply with Data Protection Laws
- Not knowingly instruct Provider to violate laws

9.3 Accuracy. Customer is responsible for the accuracy of Personal Data provided.

9.4 Customer Limitations. Customer acknowledges and agrees that:

- Provider's liability is limited by the primarily on-device architecture where >99% of data never reaches Provider's systems
- For pilot engagements, audit rights may be satisfied through existing compliance certifications (SOC 2, etc.) unless material security incidents occur
- Customer will provide reasonable advance notice (minimum 30 days) for audit requests to minimize operational disruption
- Customer shall not make unreasonable or excessive requests for reports, certifications, or evidence that would impose disproportionate burden relative to the engagement value

---

10. LIABILITY AND INDEMNIFICATION

10.1 Liability. Each party's liability arising from this DPA is subject to the limitations in the Agreement. Notwithstanding anything to the contrary in the Agreement, for material breaches of this DPA involving data breaches or violations of Data Protection Laws, the liability cap shall not be less than the greater of (a) $100,000 for pilot engagements under $50,000 in annual value, $250,000 for engagements under $250,000 in annual value, or $500,000 for larger engagements, or (b) five times the total fees paid under the applicable SOW in the 12 months preceding the event giving rise to liability, provided however that in no event shall Provider's total aggregate liability under this DPA exceed $2,000,000 (two million US dollars).

10.2 Indemnification. Each party shall indemnify the other against damages arising from its breach of this DPA, subject to the Agreement's terms.

10.3 Third Party Claims. The parties shall cooperate in defending against regulatory investigations and third-party claims.

---

11. CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

11.1 Service Provider. For CCPA purposes:

- Provider is a "Service Provider"
- Customer is a "Business"
- Provider shall Process Personal Information solely for purposes specified in the Agreement

11.2 CCPA Obligations. Provider shall:

- Not sell Personal Information
- Not retain, use, or disclose Personal Information except as permitted
- Comply with applicable CCPA obligations
- Assist Customer with consumer rights requests

11.3 Certifications. Provider certifies it understands and will comply with CCPA restrictions.

---

12. JURISDICTION-SPECIFIC TERMS

12.1 European Union/UK:

- GDPR Articles 28 and 32-36 requirements apply
- SCCs apply for international transfers
- Provider shall cooperate with lead Supervisory Authority. Provider shall notify Customer promptly of any communications with Supervisory Authorities relating to Customer's Personal Data

12.2 Australia:

- Australian Privacy Principles (APP) apply, including APP 8 for cross-border disclosures
- Provider implements reasonable steps to ensure overseas recipients comply with APPs
- Notifiable data breach scheme applies with 72-hour notification requirement
- Financial services entities: Additional APRA CPS 234 considerations where applicable

Singapore:

- Personal Data Protection Act (PDPA) compliance
- Notification of data breaches as soon as practicable where required
- Consent obligations and data transfer restrictions apply

Hong Kong:

- Personal Data (Privacy) Ordinance (PDPO) compliance
- Data breach notification per Privacy Commissioner guidance
- Direct marketing restrictions and data subject rights apply

12.3 Canada:

- PIPEDA requirements apply
- Provider acts as third-party processor
- Breach notification per applicable provincial laws

12.4 Other Jurisdictions:

- Parties shall cooperate to address jurisdiction-specific requirements
- Provider shall implement reasonable measures for compliance

---

13. GENERAL PROVISIONS

13.1 Order of Precedence. In case of conflict regarding data protection:

1. Mandatory Data Protection Laws
2. This DPA
3. The Agreement

13.2 Amendment. Amendments to this DPA require written agreement. Updates to Appendices for operational changes require at least 30 days' advance written notice to Customer, and Customer shall have the right to object to any material changes that adversely affect its data protection rights.

13.3 Severability. If any provision is invalid, the remainder continues in full force.

13.4 Term. This DPA remains effective for the duration of Processing under the Agreement.

13.5 Survival. Obligations survive as long as Provider Processes Personal Data or as required by law.

13.6 Transition Assistance. Upon termination or expiration:

- Provider shall provide reasonable transition assistance for up to 60 days
- Data export support and format documentation provided
- Reasonable professional services fees may apply for extensive transition support
- No immediate termination except for material security breaches or legal requirements

13.7 Regulatory Cooperation.

- Provider will reasonably cooperate with Customer's regulatory examinations and audits
- Advance notice provided of any regulatory investigations affecting the Services (where legally permitted)
- Support for Customer's regulatory reporting requirements with reasonable notice and scope

13.8 Force Majeure and Startup Considerations.

- Provider's obligations under this DPA may be suspended during force majeure events, including but not limited to acts of government, natural disasters, cyber attacks, or infrastructure failures beyond Provider's reasonable control
- For pilot and early-stage engagements, Provider's compliance obligations shall be proportionate to the engagement scope and Provider's resources as a growing technology company
- Customer acknowledges that certain enterprise-grade compliance features may be developed over time and agrees to work collaboratively on reasonable implementation timelines

---

SIGNATURES

CONTROLLER/CUSTOMER:

By: _____
Name: _____
Title: _____
Date: _____

Each signatory represents and warrants that they have full authority to bind their respective party to the terms of this Agreement.

PROCESSOR/PROVIDER:
Mesh Intelligent Technologies, Inc. (d/b/a pieces.app)

By: _____
Name: _____
Title: _____
Date: _____

Each signatory represents and warrants that they have full authority to bind their respective party to the terms of this Agreement.

APPENDIX 1: PROCESSING DETAILS

A. Categories of Data Subjects

- Customer's employees and contractors
- Customer's end users of Pieces software
- Authorized users/agents of Customer's development systems
- Other (subject to Processor's written approval): _____

B. Categories of Personal Data

B.1 Cloud Data Categories

Minimal Cloud Metadata (<1% - operational only):

- **Authentication State:** SSO tokens, session identifiers
- **Crash Analytics:** Error signatures, stack traces (PII scrubbed)
- **Abstract Metrics:** Feature usage counts, performance metrics (anonymized)
- **License State:** License keys, seat counts (Processor will only process license keys and seat counts to the extent necessary for license management and will not use such data for any other purpose)
- **Abuse Signals:** Rate limiting data, security flags

Ephemeral Cloud Processing (zero retention):

- **LLM Inference I/O:** Input prompts and output responses
- **Processing Context:** Temporary compute state during inference
- **No Data Storage:** Pure computational operation with immediate deletion. Provider shall ensure that no temporary or persistent storage, including logs or backups, of Customer data occurs during cloud processing, except as strictly necessary for security or compliance with applicable law, and any such storage shall be limited in scope and duration, subject to the same security and deletion protocols, and documented with notice to Customer
- **Customer Audit Option:** Storage only if explicitly requested by Customer in their Enterprise SSO Configurations. If Customer requests audit logging, Processor and Customer will agree in writing on the scope, duration, and security measures for such storage

B.2 On-Device Data (Locally Processed & Stored)

- **Source Code:** All code snippets, files, repositories
- **AI History:** Complete conversation history and context (stored locally)
- **Workflow Data:** Personal productivity data, history

- **Content Data:** All user-generated content
- **Intellectual Property:** Proprietary algorithms, trade secrets
- **Models:** Local LLM/SLM models and embeddings
- **Processed Results:** AI outputs after cloud processing (if applicable)

C. Special Categories (if applicable)

☐ None expected in cloud-hosted data ☐ May include: _____ (only with Processor's prior written consent and subject to additional safeguards as required by law)

D. Processing Purposes

Cloud Metadata (Minimal):

- Authentication state management
- License validation
- Crash analytics for stability
- Abstract usage metrics (opt-in)
- Abuse detection
- Operational monitoring

Ephemeral Cloud Processing (I/O Only):

- LLM inference computation (input → output → delete)
- No data retention or storage
- Results immediately sent to device for local persistence
- Pure computational service
- Storage only if Customer explicitly requests audit logging
- Other (subject to Processor's written approval): _____

E. Processing Operations

- Collection and storage
- Organization and structuring
- Access and retrieval
- Transmission and sharing (as authorized)
- Backup and recovery
- Deletion and destruction
- Other (subject to Processor's written approval): _____

APPENDIX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Important Note on Data Architecture

These measures apply to:

1. **Minimal cloud metadata** (<1% - authentication, crash analytics, abstract metrics)
2. **Ephemeral cloud processing infrastructure** (LLM inference with zero data retention)

Key Points:

    - 99% of actual data persists exclusively on Customer devices
- Cloud processing is purely input/output computation with no storage
- Provider has zero remote access to on-device data. Provider shall maintain technical controls to ensure that remote access to on-device data is technically impossible, and shall provide reasonable evidence of such controls upon Customer request, subject to confidentiality and security considerations
- In Air-Gapped Mode, the product operates entirely offline

Technical Measures (Cloud Infrastructure)

1. Access Control

- Multi-factor authentication (MFA) required for all cloud systems
- Role-based access control (RBAC) with quarterly reviews
- Principle of least privilege enforced
- No access to customer on-device data by design

2. Data Protection (Cloud Data Only)

- Encryption at rest (AES-256) for cloud storage
- Encryption in transit (TLS 1.2+) for API calls
- Automated PII scrubbing in crash reports. Provider shall periodically validate and document the effectiveness of automated PII scrubbing mechanisms and provide evidence of such validation to Customer upon request
- Anonymized telemetry (no identifiable data). Provider shall apply industry-standard anonymization techniques to telemetry data and, upon request, provide details of the anonymization methodology to Customer
- Secure deletion protocols for cloud data

3. System Security

- Firewalls and network segmentation
- Intrusion detection/prevention systems
- Anti-malware protection
- Vulnerability scanning and patching

4. Application Security

- Secure development lifecycle
- Code reviews and static analysis
- Dynamic application security testing
- Dependency scanning

5. Monitoring

- Security information and event management (SIEM)
- Audit logging
- Anomaly detection
- Incident response procedures

Organizational Measures

1. Personnel

- Background checks (where permitted)
- Confidentiality agreements
- Security awareness training
- Data protection training

2. Physical Security

- Secured data center facilities
- Access controls and visitor logs
- Environmental controls
- Equipment disposal procedures

3. Governance

- Information security policies
- Privacy by design principles
- Regular risk assessments
- Business continuity planning

4. Vendor Management

- Due diligence procedures
- Contractual security requirements
- Ongoing monitoring
- Risk assessments

5. Compliance

SOC 2 Type II Attestation:

- Annual audit period: July 1 - June 30
- Report delivery: September annually
- Covers Security, Availability, Confidentiality TSCs
- Provider shall provide Customer with a copy of the full SOC 2 Type II report upon request, subject to NDA, and shall promptly disclose any material findings that may impact the security or confidentiality of Customer data

Quarterly Internal Audits (performed by Information Security team):

- Q1: Access control review - All user permissions, API keys, service accounts
- Q2: Security configuration review - Infrastructure hardening, encryption validation
- Q3: Vendor/subprocessor compliance review - DPA compliance, security attestations
- Q4: Incident response & backup recovery testing
- Documentation maintained in compliance management system
- Findings tracked with 30-day remediation SLA for critical issues. If critical issues are not remediated within the 30-day SLA, Customer shall have the right to request a remediation plan. Termination for material breach shall only be permitted if the remediation plan is not implemented in good faith or the issue remains unresolved after a reasonable period

Penetration Testing:

- Annual third-party assessment by certified firm
- Covers application, infrastructure, and API security
- Critical findings remediated within 30 days
- A summary of the penetration test report, including all critical findings and remediation actions, shall be made available to Customer under NDA within 30 days of completion. Full reports may be provided at Provider's discretion, subject to additional security and confidentiality measures. Provider shall remediate all critical findings within 30 days and provide written confirmation of remediation

Continuous Compliance Monitoring:

- Vanta platform for real-time compliance tracking

- Daily automated security checks
- Monthly compliance dashboards
- Immediate alerts for configuration drift

Financial Services Alignment:

- Security controls mapped to MAS TRM Guidelines (where applicable)
- HKMA Cybersecurity Fortification Initiative considerations
- APRA CPS 234 alignment for Australian financial services
- Provider shall specify which controls are fully implemented and which are only considered, and provide supporting documentation upon Customer request

Incident Response Drills:

- Bi-annual tabletop exercises (March & September)
- Scenarios include: ransomware, data breach, service outage
- Lessons learned incorporated into IRP updates

APPENDIX 3: AUTHORIZED SUB-PROCESSORS

Infrastructure Providers

Sub-processor	**Purpose**	**Location**
Google Cloud Platform	Cloud infrastructure (primary)	United States (us-east5)
GitHub Enterprise	Code repository and CI/CD	United States

Service Providers

Sub-processor	**Purpose**	**Location**
Paddle	Payment processing (Merchant of Record)	UK/US
Descope	Authentication services	United States
Sentry	Crashlytics	United States
SendGrid	Email delivery	United States

Sub-processor	Purpose	Location
Customer.io	Email Delivery (Marketing Content Only)	United States
HubSpot	Customer Support CRM	United States
Segment	Telemetry & Crashlytics (Anonymous, Optional)	United States
Mixpanel	Telemetry & Crashlytics (Anonymous, Optional)	United States
Satismeter	In-App PMF Surveys (Rare, Optional)	United States
Hugging Face	On-device SLM/LLM Private Model Registry & Download Source (Optional)	United States
Google Workspace	Internal Email & Productivity Suite	United States

Conditional LLM Providers (Only if Customer Selects These Options)

Sub-processor	Purpose	Location	Notes
OpenAI	LLM inference (If Customer selects)	United States	Only if Customer enables OpenAI models; zero retention by default
Anthropic	LLM inference (If Customer selects)	United States	Only if Customer enables Claude models; zero retention by default
Google (Vertex/Gemini)	LLM inference (If Customer selects)	United States	Only if Customer enables Google models; zero retention by default

Note: These LLM providers are only engaged if Customer specifically selects cloud LLM options (Blended Mode, SSO-locked, or BYOK). Provider will notify Customer prior to enabling any provider with non-zero retention settings and will honor DPA §4.3 objection rights.

Provider shall notify Customer directly of any changes in accordance with the notification provisions.

Note on Subprocessors:

- This list includes material sub-processors that may process personal data in connection with the Services
- Customer acknowledges that Provider may use additional sub-processors for internal operations that do not process Customer Personal Data. For clarity, only sub-processors that process Customer Personal Data are subject to the notification and objection provisions
- Changes to sub-processors will be notified with 30 days advance notice via email to designated contacts or published on the website

---

APPENDIX 4: STANDARD CONTRACTUAL CLAUSES

Module Selection

For Controller-to-Processor transfers, the following modules apply:

- **Module Two:** Controller to Processor
- **Module Three:** Processor to Sub-processor (where applicable)

Optional Clauses

- **Clause 7:** Docking clause applies. Any new parties joining under the docking clause must be subject to prior written approval by Mesh Intelligent Technologies, Inc.
- **Clause 9(a):** Option 2 (general authorization with right to object). Objections must be based on reasonable, documented grounds related to data protection with a 30-day notice period
- **Clause 11(a):** Optional redress provision does not apply

Competent Authority

- **Supervisory Authority:** To be determined based on Customer's location and agreed upon in writing before data processing begins. For EU customers, the supervisory authority of the Customer's main establishment or place of business. For non-EU customers, not applicable for SCC purposes.
- **Courts:** Delaware state and federal courts (consistent with MSA governing law and venue provisions)

The parties shall agree in writing on the competent supervisory authority prior to the commencement of any data processing activities involving EU personal data.

Annexes to SCCs

- **Annex I:** As set out in Appendix 1 of this DPA (to be reviewed for accuracy and completeness)
- **Annex II:** As set out in Appendix 2 of this DPA (to be reviewed for accuracy and completeness)
- **Annex III:** As set out in Appendix 3 of this DPA (to be reviewed for accuracy and completeness)