

# Data Processing Agreement

Keep IT Scalable (KITS) | KITS DPA 2026 v1 | Effective October 1, 2026

---

This Data Processing Agreement (the “**DPA**”) is made by and between **Kladensky Software Development, LLC d/b/a Keep IT Scalable**, a Texas limited liability company, with its principal place of business as set forth in the MSA (“**KITS**”), and the Customer, as defined in the Master Services Agreement (“**Customer**”) (each a “**Party**,” and collectively the “**Parties**”). This DPA forms part of the Agreement (defined below), is effective for the term of the Agreement, and continues thereafter for so long as KITS Processes Personal Data on behalf of Customer. With respect to Personal Data, Customer acts as the controller (or “business”) and KITS acts as the processor (or “service provider”) under Data Protection Laws and Regulations.

## 1. Purpose of the DPA

---

The Parties have entered into a Master Services Agreement (the “**MSA**”) and may enter into one or more Statements of Work under the MSA (together with the MSA, the “**Agreement**”), under which KITS may Process Personal Data on behalf of Customer in performing the Services. This DPA sets out the Parties’ obligations with respect to that Processing. Capitalized terms used but not defined in this DPA have the meanings given in the MSA.

## 2. Definitions

---

- (a) “**Data Protection Laws and Regulations**” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, to the extent applicable: (i) Regulation (EU) 2016/679 (“**GDPR**”); (ii) the UK General Data Protection Regulation, the UK Data Protection Act 2018, and any laws amending, replacing, or superseding them (“**UK Data Protection Laws**”); (iii) the Swiss Federal Act on Data Protection (“**Swiss FADP**”); and (iv) U.S. state consumer privacy laws, including the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (together, “**CCPA**”), the Texas Data Privacy and Security Act, and any other comprehensive state consumer privacy law, in each case to the extent applicable to the Processing of Personal Data under the Agreement (collectively, “**U.S. State Privacy Laws**”).
- (b) “**Data Subject**” means the individual to whom Personal Data relates.
- (c) “**Personal Data**” means any information relating to an identified or identifiable natural person, including “personal information” and “personal data” as defined under Data Protection Laws and Regulations, that KITS Processes on behalf of Customer under the Agreement. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
- (d) “**Processing**” (or “**Process**”) means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure, or destruction.
- (e) “**Security Breach**” has the meaning given in Section 7(a).
- (f) “**Services**” has the meaning given in the MSA: professional services relating to Customer’s business applications and technology environment, as more fully described in one or more Statements of Work.

- (g) **“Standard Contractual Clauses” or “SCCs”** means the standard contractual clauses for the transfer of personal data to third countries approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as completed under Section 10(a).
- (h) **“Subprocessor”** means any third party engaged by KITS that Processes Personal Data on behalf of Customer, other than KITS personnel as described in Section 3(c)(i).

### 3. Processing of Personal Data

- (a) **Customer’s Processing of Personal Data.** Customer will Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, and Customer’s instructions for the Processing of Personal Data will comply with Data Protection Laws and Regulations. Customer is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.
- (b) **KITS’s Processing of Personal Data.** KITS will Process Personal Data only on behalf of and in accordance with Customer’s documented instructions and in relation to the Agreement and its purpose (the **“Purpose”**), and will treat Personal Data as Confidential Information. By entering into this DPA, Customer instructs KITS to Process Personal Data in accordance with the Purpose. Customer may issue additional instructions to KITS, and KITS will promptly comply with such additional instructions, provided that they: (i) comply with Data Protection Laws and Regulations; (ii) are issued by Customer in writing and with sufficient advance notice for KITS to review, consider, and act on them; (iii) do not provide KITS with additional sensitive or special categories of Personal Data that impose data security or data protection obligations on KITS beyond those contemplated in the Agreement; and (iv) are instructions KITS has the means and authority to carry out. To the extent KITS expects to incur charges or fees not contemplated by the Agreement in connection with any additional instructions, the Parties will negotiate in good faith as to which Party bears those costs.
- (c) **Subprocessors.**
  - (i) Customer authorizes KITS to engage the Subprocessors listed in Annex III. Individual independent contractors who perform Services under KITS’s direction and supervision are KITS personnel, not Subprocessors, and are subject to the personnel obligations in Section 5 and Annex II. KITS will identify any such contractor assigned to Customer’s engagement upon Customer’s request. A contractor that is a business entity rather than an individual is a Subprocessor.
  - (ii) KITS will bind each Subprocessor by written agreement to data protection obligations no less protective than those in this DPA, to the extent applicable to the services the Subprocessor provides. KITS remains responsible to Customer for each Subprocessor’s performance of those obligations.
  - (iii) KITS will notify Customer in writing (email sufficient) at least fifteen (15) days before engaging a new Subprocessor to Process Customer’s Personal Data.
  - (iv) Customer may object in writing, on reasonable data protection grounds, within that notice period. The Parties will discuss the objection in good faith, and KITS may propose alternatives, such as not using that Subprocessor for Customer’s Services. If the objection is not resolved within thirty (30) days, Customer may terminate only the Services that cannot be performed without that Subprocessor, and KITS will refund any prepaid fees for those unperformed Services. Customer remains responsible for fees for Services performed through the date of termination.
- (d) **Unlawful Instructions.** KITS will promptly inform Customer if, in KITS’s opinion, an instruction from Customer infringes Data Protection Laws and Regulations, and KITS may suspend performance of such instruction until Customer confirms or modifies it in writing.
- (e) **Details of Processing.** The subject matter, duration, nature, and purpose of the Processing, and the types of Personal Data and categories of Data Subjects, are described in Annex I.B, which applies to all Processing under this DPA.

- (f) **AI Tools.** KITS may use the AI tools listed in Annex III in performing the Services, including tools that connect to the Customer IT Environment through integrations authorized by Customer. KITS will: (i) use AI tools only under business or enterprise terms that prohibit the provider from using Customer's Personal Data to train its models; (ii) connect an AI tool to the Customer IT Environment only with Customer's authorization, with access limited to what is necessary to perform the Services; (iii) not input Customer Personal Data into an AI tool except as necessary to perform the Services; and (iv) have KITS personnel review AI-generated output before incorporating it into Work Product. Customer may prohibit or limit the use of AI tools, or any specific AI tool, in a SOW or by written notice. In that case the Parties will agree on any resulting changes to scope, timeline, or fees through a Change Order.

## 4. Rights of Data Subjects

---

- (a) **Correction, Blocking, and Deletion.** To the extent Customer does not have the ability to correct, amend, block, or delete Personal Data as required by Data Protection Laws and Regulations, KITS will comply with any commercially reasonable written request by Customer to facilitate such actions, to the extent KITS is legally permitted to do so. Customer is responsible for any costs arising from KITS's assistance.
- (b) **Data Subject Requests.** KITS will, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise any right under Data Protection Laws and Regulations, including access to, correction, amendment, or deletion of that person's Personal Data. KITS will not respond to any such request without Customer's prior written consent, except to confirm that the request relates to Customer. KITS will provide Customer with commercially reasonable cooperation and assistance in handling such requests, to the extent legally permitted and to the extent Customer does not have access to the relevant Personal Data. Customer is responsible for any costs arising from KITS's assistance.

## 5. KITS Personnel

---

- (a) **Confidentiality.** KITS will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements, and that such confidentiality obligations survive the end of their engagement.
- (b) **Reliability.** KITS will take commercially reasonable steps to ensure the reliability of any KITS personnel engaged in the Processing of Personal Data.
- (c) **Limitation of Access.** KITS will ensure that access to Personal Data is limited to those personnel performing the Services, or related oversight of the Services, in accordance with the Agreement.
- (d) **Data Protection Contact.** KITS has designated a person responsible for overseeing its data protection responsibilities and obligations, who may be reached at [legal@keepitscalable.com](mailto:legal@keepitscalable.com).

## 6. Security

---

KITS maintains appropriate administrative, physical, and technical safeguards for the protection of the security (including protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage), confidentiality, and integrity of Personal Data, including the measures described in Annex II.

## 7. Security Breach Management and Notification

---

- (a) **"Security Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by KITS or its Subprocessors under the Agreement.

- (b) KITS maintains security incident management procedures. KITS will notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Security Breach. KITS will promptly investigate any reasonably suspected Security Breach.
- (c) KITS's notice will describe, to the extent then known: the nature of the Security Breach; the categories and approximate number of Data Subjects and records affected; its likely consequences; the measures taken or proposed to address it; and a point of contact. Where information is not available at the time of notice, KITS will provide it in phases as it becomes available.
- (d) KITS will take reasonable steps to contain and remediate a Security Breach and will reasonably cooperate with Customer's investigation. Customer, as controller, is responsible for any notifications to supervisory authorities or Data Subjects. KITS will not make such notifications on Customer's behalf unless required by law or instructed by Customer in writing.
- (e) Where a Security Breach occurs within the Customer IT Environment and is not caused by KITS's breach of this DPA, KITS will reasonably cooperate with Customer, and any such assistance is billable at KITS's then-current rates.
- (f) KITS's notification of or response to a Security Breach is not an acknowledgment of fault or liability.

## 8. Assistance with Compliance

Taking into account the nature of the Processing and the information available to KITS, KITS will provide Customer reasonable assistance with Customer's obligations relating to security of Processing, notification of Security Breaches, data protection impact assessments, and prior consultation with supervisory authorities, in each case to the extent required by Data Protection Laws and Regulations. Customer will reimburse KITS for such assistance at KITS's then-current rates, except where the assistance is required due to KITS's breach of this DPA.

## 9. Return or Deletion of Personal Data

Upon completion or termination of the Services, or upon Customer's written request, KITS will, at Customer's election, delete or return all Personal Data in KITS's possession or control, including any copies held by Subprocessors, within thirty (30) days, and will certify deletion in writing upon request. Personal Data residing in the Customer IT Environment remains under Customer's control; KITS's obligation with respect to that data is to cease accessing it and cooperate with Customer's removal of KITS access. If applicable law requires KITS to retain any Personal Data, KITS will continue to protect it under this DPA and Process it only as required by such law. Personal Data in routine backups will be deleted in the ordinary course of backup rotation and remains protected under this DPA until deleted.

## 10. International Data Transfers

- (a) **EU Transfers.** To the extent KITS Processes Personal Data that is subject to the GDPR and is transferred to KITS in a country that has not been recognized by the European Commission as providing an adequate level of protection, the Parties agree to the SCCs, Module Two (controller to processor), which are incorporated into this DPA by reference, with Customer as the data exporter and KITS as the data importer, and completed as follows: (i) Clause 7 (docking clause) applies; (ii) in Clause 9, Option 2 (general written authorization) applies, and the time period for prior notice of Subprocessor changes is fifteen (15) days, consistent with Section 3(c); (iii) in Clause 11, the optional language does not apply; (iv) in Clause 13, the competent supervisory authority is as set out in Annex I.C; (v) in Clause 17, Option 1 applies, and the SCCs are governed by the law of Ireland; (vi) in Clause 18(b), disputes will be resolved before the courts of Ireland; and (vii) Annexes I, II, and III of the SCCs are completed by Annexes I, II, and III of this DPA.

- (b) **UK Transfers.** To the extent KITS Processes Personal Data that is subject to UK Data Protection Laws and is transferred to KITS in a country not recognized as adequate under UK Data Protection Laws, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0, in force 21 March 2022) (the “**UK Addendum**”) is incorporated into this DPA by reference and completed as follows: (i) in Table 1, the Parties’ details and key contacts are as set out in the Agreement and Annex I.A; (ii) in Table 2, the Addendum EU SCCs are the SCCs as completed under Section 10(a); (iii) in Table 3, the Appendix Information is set out in Annexes I, II, and III of this DPA; and (iv) in Table 4, neither Party may end the UK Addendum under its Section 19.
- (c) **Swiss Transfers.** To the extent KITS Processes Personal Data that is subject to the Swiss FADP and is transferred to KITS in a country not recognized as adequate under the Swiss FADP, the SCCs apply as completed under Section 10(a), with the following modifications: (i) references to the GDPR are read as references to the Swiss FADP to the extent the transfer is subject to it; (ii) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and (iii) the term “Member State” in Clause 18(c) does not exclude Data Subjects in Switzerland from bringing legal proceedings in their place of habitual residence.
- (d) **Supplementary Measures.** KITS will reasonably cooperate with Customer in any assessment of whether the laws of the country to which Personal Data is transferred provide a level of protection essentially equivalent to that required under the GDPR, UK Data Protection Laws, or the Swiss FADP, as applicable. If Customer reasonably determines in good faith, or a competent supervisory authority or court determines, that such protection is not being provided, the Parties will agree on supplementary measures. If the Parties cannot agree on supplementary measures that provide the required protection, Customer may suspend the affected transfer and terminate the affected Services on written notice, without penalty, subject to payment for Services performed through the effective date of termination.
- (e) **Subprocessors.** This Section 10 applies to any transfer of Personal Data to a Subprocessor, and KITS will ensure that any such transfer is subject to appropriate safeguards under Data Protection Laws and Regulations.

## 11. U.S. State Privacy Laws

To the extent U.S. State Privacy Laws apply to Personal Data Processed under the Agreement, KITS acts as Customer’s “service provider,” “contractor,” or “processor” (as those terms are defined under the applicable law), and KITS will:

- (a) not sell or share Personal Data, as the terms “sell” and “share” are defined under U.S. State Privacy Laws;
- (b) not retain, use, or disclose Personal Data for any purpose other than performing the Services, including any commercial purpose other than performing the Services, or as otherwise permitted by U.S. State Privacy Laws;
- (c) not retain, use, or disclose Personal Data outside the direct business relationship between KITS and Customer;
- (d) not combine Personal Data with personal information KITS receives from or on behalf of any other person, except as permitted by U.S. State Privacy Laws;
- (e) comply with the obligations that apply to it under U.S. State Privacy Laws and provide the same level of privacy protection as those laws require;
- (f) notify Customer if KITS determines it can no longer meet its obligations under U.S. State Privacy Laws;
- (g) ensure that each person Processing Personal Data is subject to a duty of confidentiality, and require any Subprocessor to comply with obligations consistent with this Section 11 by written contract;

- (h) where KITS receives deidentified data, maintain it in deidentified form and not attempt to reidentify it; and
- (i) permit Customer, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

KITS's obligations to delete or return Personal Data and to make information available to demonstrate compliance are set out in Section 9 and Section 12. KITS certifies that it understands and will comply with the restrictions in this Section 11.

## 12. Audits

- (a) **Documentation.** Upon Customer's written request, no more than once per calendar year, KITS will provide information reasonably necessary to demonstrate its compliance with this DPA, including completing a reasonable written security questionnaire and providing relevant policies, which Customer will treat as KITS's Confidential Information.
- (b) **Audits and Inspections.** Customer, or an independent auditor bound by confidentiality obligations and not a competitor of KITS, may conduct an audit or inspection of KITS only if: (i) required by a supervisory authority or applicable law; (ii) following a Security Breach caused by KITS; or (iii) the information provided under Section 12(a) is not sufficient to reasonably demonstrate KITS's compliance with Data Protection Laws and Regulations. Except where a supervisory authority requires otherwise, any such audit will: occur no more than once per calendar year; be conducted on at least thirty (30) days' written notice, during normal business hours, and remotely where practicable; follow a scope mutually agreed in advance; and be limited to KITS's systems and records relating to Customer's Personal Data, excluding information relating to KITS's other customers.
- (c) **Costs.** Each Party bears its own costs of any audit. Customer will reimburse KITS's time spent supporting an audit under Section 12(b) at KITS's then-current rates, unless the audit reveals material non-compliance by KITS with this DPA.
- (d) **Findings.** If an audit identifies material non-compliance by KITS, KITS will promptly prepare and implement a reasonable plan to remediate it.
- (e) **Subprocessors.** Upon request, KITS will provide information regarding its Subprocessors' compliance with obligations consistent with this DPA and will reasonably assist Customer in exercising any audit rights with respect to a Subprocessor.

## 13. Limitation of Liability

Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability in Section 8 (Limitation of Liability & Damage Waivers) of the MSA. Any reference in that Section to a Party's liability means that Party's aggregate liability under the MSA, all SOWs, and this DPA together. Nothing in this Section limits either Party's liability to Data Subjects under the SCCs, or any liability that cannot be limited under applicable law.

## 14. Version; Updates

This DPA is identified as **KITS DPA 2026 v1**. The version of this DPA in effect on the date Customer executes the MSA governs, unless replaced as provided in this Section 14. KITS may publish updated versions from time to time at <https://www.keeptscalable.com/agreements.html> and will keep prior versions available upon request. An updated version applies to Customer only: (a) upon mutual written agreement; or (b) upon the next renewal of the MSA, if KITS gives Customer at least thirty (30) days' written notice before the renewal date and Customer does not object in writing before that date. If Customer objects, the prior version continues to apply. Notwithstanding the foregoing,

KITS may (i) update Annex III in accordance with Section 3(c), and (ii) make changes required to comply with changes in Data Protection Laws and Regulations or to adopt updated standard contractual clauses issued by a competent authority, upon written notice to Customer.

## 15. Miscellaneous

---

- (a) **Entire Agreement.** This DPA constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior understandings regarding that subject matter, whether written or oral.
- (b) **Order of Precedence.** In the event of a conflict: (i) the SCCs and the UK Addendum prevail over this DPA and the MSA, to the extent they apply; (ii) this DPA prevails over the MSA with respect to the Processing of Personal Data; and (iii) notwithstanding (ii), the MSA governs all matters of liability, as provided in Section 13.
- (c) **Assignment.** This DPA binds and benefits the Parties and their permitted successors and assigns, and may be assigned only together with the MSA in accordance with Section 12.1 (Assignment) of the MSA.
- (d) **Amendment and Waiver.** Except as provided in Section 14, no amendment of this DPA is binding unless in writing and signed by both Parties. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach.
- (e) **Severability; Language.** If a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect. If this DPA is translated into languages other than English, the English version controls.
- (f) **Survival.** Provisions of this DPA that by their nature are to be performed or enforced following termination of the Agreement survive such termination, and this DPA continues to apply for so long as KITS retains any Personal Data.

## 16. Authority of Signatories

---

Each person signing the Agreement represents and warrants that he or she is duly authorized and has legal capacity to bind the Party on whose behalf he or she signs to this DPA.

## Annex I – Description of Processing

---

### A. List of Parties

**Data exporter / controller:** Customer, as identified in the MSA, with the contact information set out in the notices section of the MSA. Activities relevant to the transfer: receiving the Services. Signature and date: as set out in the MSA.

**Data importer / processor:** Kladensky Software Development, LLC d/b/a Keep IT Scalable, with the address set forth in the MSA; contact: [legal@keepitscalable.com](mailto:legal@keepitscalable.com). Activities relevant to the transfer: performing the Services. Signature and date: as set out in the MSA.

### B. Description of Processing and Transfer

**Categories of Data Subjects:** As determined by Customer's instructions and the nature of the Services, natural persons who are Customer's employees; directors or officers; shareholders; suppliers, vendors, or contractors; leads, prospects, or customers; and end users of Customer's software or websites.

**Categories of Personal Data:** As determined by Customer, the categories of Personal Data contained in the business applications and systems within the scope of the Services, which typically include contact details, account and user identifiers, and business relationship and transaction records.

**Sensitive data:** None anticipated. Customer is solely responsible for disclosing to KITS in advance the existence of any sensitive data within the scope of the Services, meaning Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; genetic data; biometric data used to uniquely identify a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation. Protected health information is prohibited as provided in the MSA.

**Frequency of transfer:** As needed to perform the Services during the term of the applicable SOW(s).

**Nature of Processing:** Accessing, viewing, querying, configuring, migrating, transforming, validating, integrating, and testing Personal Data within the Customer IT Environment, including through the AI tools listed in Annex III where authorized by Customer, as necessary to perform the Services.

**Purpose of Processing:** For KITS to perform or deliver the Services.

**Retention:** For the duration necessary to perform the Services, after which Personal Data is deleted or returned in accordance with Section 9.

**Transfers to Subprocessors:** Same subject matter, nature, and duration as above, limited to the services each Subprocessor provides as described in Annex III.

### C. Competent Supervisory Authority

For purposes of the SCCs, the competent supervisory authority is: (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the territorial scope of the GDPR and has appointed a representative, the supervisory authority of the Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the territorial scope of the GDPR without being required to appoint a representative, the supervisory authority of the Member State in which the Data Subjects are predominantly located. For Personal Data subject to UK Data Protection Laws or the Swiss FADP, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner, as applicable.

## Annex II – Technical and Organizational Measures

---

### A. Data Handling Model

1. Access to Personal Data is provisioned and controlled by Customer within the Customer IT Environment. KITS does not host or store Customer Personal Data on KITS systems unless expressly agreed in a SOW.
2. KITS personnel access only the portions of the Customer IT Environment necessary to perform the Services, on a need-to-know basis.
3. Files that may contain Personal Data are shared and stored in Customer-controlled environments rather than KITS systems.
4. KITS requests that Customer remove KITS access upon completion of the Services, and KITS deletes any locally held copies of Personal Data at that time.

### B. Personnel Controls

1. All KITS personnel (employees and contractors) sign written confidentiality agreements before accessing Customer data, and those obligations survive the end of their engagement.
2. Where permitted by applicable law, KITS personnel are subject to background checks as a condition of engagement.
3. All KITS personnel complete security awareness training upon engagement and monthly thereafter.
4. All KITS personnel acknowledge and follow KITS's written acceptable use and information security policy.

### C. Technical Controls

1. Full-disk encryption is enabled on all devices used to perform the Services.
2. Credentials for Customer systems are stored in an encrypted password manager and are not shared through email, chat, or other unencrypted channels.
3. Multi-factor authentication is enabled on KITS email and on all accounts used to access Customer systems, wherever the system supports it.
4. Endpoint protection software (antivirus or endpoint detection and response) is installed and kept current on all devices used to perform the Services.
5. Operating systems and software on these devices are kept current with security updates.

### D. AI Tools

1. AI tools are used only as described in Section 3(f) of this DPA, under business or enterprise terms that prohibit training on Customer data.

### E. Incident Response

1. KITS maintains a written incident response procedure and will notify Customer of a Security Breach as provided in Section 7.
2. KITS periodically reviews its information security practices for improvement.

## Annex III – List of Subprocessors

---

Customer has authorized the use of the following Subprocessors. Individual independent contractors working under KITS's direction and supervision are KITS personnel and are not listed here (see Section 3(c)(i)).

1. **Google LLC:** Google Workspace (email, document storage, collaboration) and Gemini; United States.
2. **Anthropic, PBC:** Claude (AI assistant), including connectors to Customer business applications when authorized by Customer; United States.
3. **Salesforce, Inc.:** MeshMesh (AI agent for Salesforce configuration and operations), connecting to Customer's Salesforce environment when authorized by Customer; United States.