Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is entered into as of the Effective Date by and between:

CheckIT Technologies LLC, a California limited liability company with its principal place of business at 144 Via Bandolero , Arroyo Grande CA 93420 ("Processor" or "CheckIT"),

and

You, the subscribing customer of the CheckIT Invoice platform ("Controller" or "Customer").

This DPA supplements and is incorporated by reference into the CheckIT Invoice Terms of Service (the "Agreement"). In the event of any conflict between this DPA and the Agreement, this DPA will control with respect to data protection matters.

---

1. Definitions

1.1 **"Applicable Law"** means all data protection and privacy laws that apply to the Processing of Personal Data under this DPA, including but not limited to:

- California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"),
- Other U.S. state privacy laws (including Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, and Virginia CDPA),
- Any implementing, successor, or equivalent laws.

1.2 **"Personal Data"** means any information relating to an identified or identifiable natural person that is Processed by Processor on behalf of Controller pursuant to the Agreement.

1.3 **"Processing"** (and "Process") has the meaning given in CCPA/CPRA Art. and includes any operation performed on Personal Data.

1.4 **"Subprocessor"** means any third party engaged by Processor to Process Personal Data on behalf of Controller.

---

2. Purpose & Scope

2.1 This DPA governs Processor's Processing of Personal Data submitted by Controller in connection with use of the CheckIT Invoice platform for financial document verification.

2.2 Processor shall Process Personal Data only:

- On documented instructions from Controller (this DPA and the Agreement constitute Controller's instructions);
- As necessary to provide the Services;
- In compliance with Applicable Law.

2.3 **Support & Troubleshooting Access.** Controller acknowledges and authorizes that Processor may access and review uploaded documents (including invoices, purchase orders, and quotes) solely to:

- Diagnose, reproduce, and resolve technical or functional issues reported by Controller;
- Verify accuracy and completeness of Processing; and
- Provide training or guidance requested by Controller's authorized personnel.
  Such access is restricted to authorized personnel subject to confidentiality and security obligations.

---

3. Roles & Responsibilities

3.1 Controller is solely responsible for the lawfulness of the Personal Data it submits and ensuring it has the rights and consents necessary for Processor's Processing.

3.2 Processor shall:

- Process Personal Data only as set forth in this DPA and the Agreement;
- Ensure all personnel authorized to Process Personal Data are bound by confidentiality;
- Implement and maintain appropriate technical and organizational measures as described in Section 6.

---

4. Data Types & Processing

- **Nature of Processing:** OCR, data extraction, AI discrepancy detection, reporting, and dispute drafting.

- **Categories of Data Subjects:** Vendors, contractors, employees, or other individuals whose data appears in financial documents.
- **Categories of Personal Data:** Names; business addresses; invoice dates; financial terms; tax identifiers; contact details; and other elements appearing in documents.

---

5. Subprocessors

5.1 Controller authorizes Processor to engage the following Subprocessors:

Subprocessor	Purpose	Location
Microsoft Azure	OCR, storage, compute, telemetry	U.S.
OpenAI, L.L.C.	NLP for dispute suggestions and summaries	U.S.
Resend	Email delivery for dispute summaries	U.S

5.2 Processor shall notify Controller at least **30 days** before appointing a new Subprocessor, allowing Controller the right to object on reasonable grounds.

---

6. Security Measures

Processor shall maintain administrative, physical, and technical safeguards consistent with SOC 2 Type II and ISO 27001 principles, including:

- Encryption: TLS 1.2+ in transit; AES-256 at rest.
- Access Control: Role-based access, least privilege, MFA for admin accounts.
- Network Security: Firewalls, IDS/IPS, vulnerability scans.
- Physical Security: Data centers certified under SOC 2/ISO 27001.
- Monitoring & Logging: Logs retained at least 12 months.
- Incident Response: Documented procedures, drills, and 24/7 escalation.

---

7. Data Subject Rights

7.1 Processor shall promptly notify Controller of any data subject request received.
7.2 Processor will assist Controller in fulfilling data subject rights requests (access, erasure,

correction, portability, restriction, objection) under Applicable Law.
7.3 Requests may be submitted to **privacy@checkitinvoice.com**.

---

8. Breach Notification

8.1 In the event of a confirmed Personal Data Breach, Processor shall notify Controller **without undue delay** and no later than **72 hours** after becoming aware.

8.2 Such notice will include: (a) description of the breach; (b) categories of data and approximate number of affected individuals; (c) likely consequences; and (d) proposed remediation measures.

8.3 Processor shall cooperate with Controller in regulatory notifications and communication with data subjects as required.

---

9. Audit Rights

9.1 Controller may audit Processor's compliance with this DPA once annually, subject to:

- 30 days' written notice;
- During regular business hours;
- Without disruption to Processor's operations;
- Under confidentiality obligations.

9.2 Processor may fulfill this requirement by providing a current SOC 2 Type II or ISO 27001 certificate.

---

10. Data Retention & Deletion

10.1 Upon termination or expiration of the Agreement, Processor shall delete or return all Personal Data within **30 days**, unless required by law to retain it.

10.2 Residual copies in backups will be deleted in accordance with standard retention cycles, not exceeding **90 days**.

10.3 During the beta phase of the Service, Processor will use commercially reasonable efforts to retain Customer Data on a per-account basis as the platform evolves toward general availability. Customer acknowledges that, consistent with standard beta practices in software development, data

persistence and continuity may be subject to change and certain usage expectations may differ from the production environment.

10.4 Indemnification related to data retention and deletion obligations under this Section is expressly limited to the scope of Section 11 (Indemnity) and subject to the limitations set forth in Section 12 (Liability & Insurance).

---

11. Indemnity

Each party shall indemnify the other against regulatory fines and third-party claims arising from its own breach of this DPA.

---

12. Liability & Insurance

Processor’s liability for breaches of this DPA is subject to the Agreement’s limitations of liability.

---

13. Term & Termination

This DPA remains in effect for the duration of the Agreement and survives termination to the extent required to satisfy obligations under Sections 8 and 11.

---

14. Governing Law

This DPA is governed by the laws and dispute resolution provisions specified in the Agreement.

IN WITNESS WHEREOF, the parties agree this DPA is effective as of the date the Customer accepts the CheckIT Terms of Service or signs a separate agreement referencing this DPA.