Documo Data Processing Agreement (US)

Effective Date: [Date]

Parties

1. Please reference the Order Agreement for opt-in and customer details (**Client**); and
2. Documo, Inc., a company incorporated in Delaware, United States, with a place of business at 919 N Market St, Suite 950, Wilmington, DE 19801 (the "**Processor**" or "**Documo**"), each a "Party" and together the "Parties."

Background

(A) The Client and the Processor are party to the Subscription Agreement referenced in the Order Agreement (the "**Agreement**"). For the avoidance of doubt, the Agreement includes any other agreement that is incorporated into the Agreement or is entered into in connection with the Agreement.

(B) The Parties agree that in order to comply with applicable US Data Protection Laws and to ensure the proper processing and security of Client Personal Data, they are entering into and will comply with the terms of this Data Processing Agreement ("**DPA**").

Agreed Terms

1. Definitions

In this DPA:

Client Personal Data means the Personal Data Processed by Processor pursuant to the Agreement and this DPA.

Data Subject means an identified or identifiable natural person about whom Personal Data relates.

Personal Data means any information relating to an identified or identifiable natural person, including but not limited to names, contact information, identification numbers, location data, online identifiers, health information, financial information, and any other data that can be used to identify an individual, either alone or in combination with other information.

Processing or **Process** means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

Protected Health Information or **PHI** has the meaning set forth in 45 CFR § 160.103 under the Health Insurance Portability and Accountability Act ("HIPAA").

Security Breach means the unauthorized acquisition, destruction, loss, alteration, or unauthorized access to, disclosure, use, or modification of Client Personal Data that compromises the security, confidentiality, or integrity of Client Personal Data.

Services shall have the meaning defined in the Agreement

Sub-processor means any third party engaged by Processor to Process Client Personal Data on behalf of the Client.

US Data Protection Laws means applicable US federal and state laws governing the Processing of Personal Data, to the extent such laws impose obligations on Processor in its role as a data processor or service provider.

2. Processing of Personal Data

2.1 Instructions for Processing. The Client instructs the Processor to Process Client Personal Data as reasonably necessary for the provision of the Services and consistent with the Agreement. The details of such Processing are set out in Schedule 1 (Data Processing Activities).

2.2 Incorporation. This DPA is incorporated into and shall be governed by the terms of the Agreement. If any provision of the Agreement conflicts with this DPA, this DPA shall take precedence to the extent of the inconsistency.

2.3 Processor Obligations. The Processor shall:

2.3.1 Only Process Client Personal Data as set forth in this DPA, the Agreement, and other documented instructions of the Client;

2.3.2 Ensure that Processor personnel who Process Client Personal Data are bound by obligations of confidentiality or are under appropriate statutory obligations of confidentiality;

2.3.3 Ensure that personnel who Process Client Personal Data receive training in data protection and privacy practices, with such training repeated or updated at least annually, as required by US Data Protection Laws;

2.3.4 Taking into account the nature of the Processing and information available to Processor, provide reasonable assistance to Client in meeting Client's obligations under US Data Protection Laws, including assistance with security assessments, privacy impact assessments, and responding to regulatory inquiries.

2.3.5 Implement appropriate technical and organizational security measures to protect Client Personal Data. Such measures shall include, as appropriate:

- Encryption of Personal Data at rest and in transit;
- Regular security assessments and testing;
- Access controls and authentication mechanisms;
- Logging and monitoring of data access;
- Incident response procedures;
- Regular backup and disaster recovery capabilities.

2.4 US Data Storage. Under this agreement, all Client Personal Data shall be processed and stored exclusively within the United States as set forth by the client's configuration settings.

2.5 HIPAA Considerations. Where Client Personal Data includes PHI, the Parties acknowledge that a separate Business Associate Agreement governs the specific HIPAA requirements. This DPA does not replace the Business Associate Agreement.

2.6 Client Obligations. Client shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with US Data Protection Laws. Client shall ensure that the processing of Personal Data in accordance with Client's instructions will not cause Processor to be in breach of the US Data Protection Laws. Client is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Processor by or on behalf of Client, (ii) the means by which Client acquired any such Personal Data, and (iii) the instructions it provides to Processor regarding the Processing of such Personal Data. Client shall not provide or make available to Processor any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Processor from all claims and losses in connection therewith.

3. Sub-processing of Personal Data

3.1 Sub-processor Authorization. Current Sub-processors are listed at https://www.documo.com/subprocessors. Processor may add additional Sub-processors by updating this list. The client may subscribe to notifications of Sub-processor changes at the same URL. Client further agrees that Processor may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Client.

3.2 Sub-processor Agreements. Processor shall impose data protection obligations on each Sub-processor that are substantially similar to those set out in this DPA, providing sufficient guarantees to implement appropriate technical and organizational security measures.

3.3 Client Objection. If Client objects to a new Sub-processor, Client must notify Processor at legal@documo.com within thirty (30) days of notification. The Parties will work in good faith to address Client's concerns, which may include migration to an alternative Sub-processor.

4. Data Subject Rights

4.1 Assistance with Requests. Processor shall:

4.1.1 Immediately refer to the Client any individual who contacts Processor seeking to exercise rights regarding their Personal Data;

4.1.2 Promptly notify Client if Processor receives any such request, except where prohibited by law or court order; and

4.1.3 Provide reasonable cooperation and assistance to enable Client to respond to Data Subject requests in accordance with US Data Protection Laws, including requests for:

- Access to Personal Data;
- Correction or deletion of Personal Data;
- Restriction of Processing;
- Data portability (where applicable);
- Opt-out of certain data uses (where applicable under state laws).

5. Security Breach Notification

5.1 Notification Obligations. Processor shall:

5.1.1 Notify Client in writing of any Security Breach without undue delay after Processor confirms the existence of a Security Breach;

5.1.2 Take reasonable steps to investigate each Security Breach and assist Client with any investigation Client chooses to conduct;

5.1.3 Take reasonable steps requested by Client to limit, stop, or remedy the Security Breach.

5.2 Breach Details. The initial notification under clause 5.1.1 shall, to the extent known to Processor:

5.2.1 Describe the nature of the Security Breach, including categories and approximate numbers of affected Data Subjects and Personal Data records;

5.2.2 Provide contact information for Processor's designated security contact;

5.2.3 Describe likely consequences of the Security Breach;

5.2.4 Describe measures taken or proposed to address the Security Breach.

5.3 Follow-up Information. Following initial notification, Processor shall provide additional information reasonably necessary to enable Client to:

- Meet any notification obligations to regulatory authorities or affected individuals;
- Comply with applicable US Data Protection Laws;

6. Privacy and Security Assessments

6.1 Reasonable Assistance. Processor shall provide reasonable assistance to Client with privacy impact assessments, security risk assessments, and consultations with regulatory authorities that are reasonably determined to be required under US Data Protection Laws.

7. Data Retention and Deletion

7.1 Post-Termination. Within thirty (30) days after termination or expiration of Services involving Processing of Personal Data (the "**Cessation Date**"), Processor shall, at Client's direction:

- Securely delete or destroy all Client Personal Data; or
- Return a complete copy of Client Personal Data to Client in a mutually agreed format, followed by secure deletion.

7.2 Legal Retention. If applicable law requires Processor to retain certain Client Personal Data, Processor shall to the extent legally permitted, inform Client and maintain the confidentiality of such data, restricting Processing to only what is legally required.

8. Audit Rights

8.1 Audit Cooperation. Processor shall:

8.1.1 Provide Client with information reasonably requested to demonstrate compliance with this DPA, including results of relevant security audits or certifications (e.g., SOC 2);

8.1.2 Upon Client's request, but no more than once annually, provide a written certification that Processor has maintained privacy and security processes in compliance with this DPA.

8.2 Confidentiality. Processor may redact or withhold proprietary or confidential information unrelated to obligations under this DPA from audit materials.

9. General Terms

9.1 Governing Law. This DPA and any disputes arising from it shall be governed by and construed in accordance with the laws of the State of Delaware, United States, without regard to its conflict of law provisions.

9.2 Jurisdiction. Each Party irrevocably agrees that the courts of Delaware, United States, shall have exclusive jurisdiction over any disputes arising from this DPA.

9.3 Order of Precedence. Nothing in this DPA reduces Processor's obligations under the Agreement. In the event of inconsistencies between this DPA and other agreements between the Parties, this DPA shall prevail to the extent of the inconsistency.

9.4 Severability. If any provision of this DPA is invalid or unenforceable, the remainder shall remain valid and in force. Invalid provisions shall be amended to ensure validity while preserving the Parties' intent or, if not possible, construed as if never included.

9.5 Notices. Communications required under this DPA shall be made in accordance with the Agreement. Security Breach notifications under Section 5 shall be made by the most expedient method available to legal@documo.com, followed by written confirmation.

9.6 Amendment. This DPA may only be amended by written agreement signed by authorized representatives of both Parties.

SCHEDULE 1: Data Processing Activities

Data Subjects

Personal Data Processed under this DPA concerns the following categories of Data Subjects:

- Business customers and end users
- Employees and personnel
- Website visitors and marketing contacts
- Vendors and business partners
- Support and service recipients
- Partners and collaborators

Categories of Personal Data

Personal Data Processed may include:

- **Identity Data:** Names, titles, professional credentials
- **Contact Data:** Email addresses, phone numbers, postal addresses, fax numbers
- **Demographic Data:** Age, date of birth, gender
- **Professional Data:** Job title, employer information, professional licenses
- **Financial Data:** Payment information, billing details
- **Technical Data:** IP addresses, device identifiers, system logs
- **Communications Data:** Fax transmissions, email content, electronic signatures
- **Document Content:** Uploaded files, scanned documents, form submissions

Nature and Purpose of Processing

Processing activities include:

- Transmission and receipt of fax communications
- Transmission and receipt of digital communications
- Optical character recognition (OCR) and document processing
- Document classification and data extraction
- Electronic signature processing and verification
- Storage and retrieval of documents and data
- System logging and security monitoring
- Customer support and technical assistance
- Service improvement and quality assurance

Duration of Processing

Processing will continue for the duration specified in the Order Agreement, plus the retention period required for data deletion obligations under Section 7.

DOCUMO, INC.	**COUNTERPARTY**
Signature:_____	Signature:_____
Date: _____	Date: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____