Simpson Healthcare Data Processing Agreement

This Data Processing Agreement ("DPA") supplements the Master Service Agreement between Simpson Healthcare Executives, LLC (hereinafter "Simpson Healthcare") and [Customer], (hereinafter "Customer") and, or other agreement between Customer and Simpson Healthcare governing Customer's use of the Service Offerings (collectively, the "Agreement") when the GDPR applies to your use of our Services to process Customer Data. This DPA is an agreement between you and the entity you represent ("Customer", "you" or "your") and Simpson Healthcare under the Agreement ("Simpson Healthcare", "We", "Our", "Data Processor"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in in the definitions section of this DPA.

GENERAL TERMS.

a) The parties agree that this DPA shall replace any existing DPA or other contractual provisions pertaining to the subject matter contained herein the parties may previously have entered in connection with Services.

b) Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail.

c) Any claims brought under or in connection with this DPA are subject to the terms and conditions, including but not limited to the exclusions and limitations of liability, set forth in the Agreement.

ROLES OF PARTIES; CUSTOMER OBLIGATIONS

a) The Parties acknowledge and agree that for purposes of this DPA, Simpson Healthcare **is a Processor** of Customer Personal Data, and that **Customer is a Controller.**

b) Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its Processing of Customer Personal Data and any Processing instructions it issues to Simpson Healthcare; and (ii) it has provided all notices, and obtained all consents and rights, necessary under Data Protection Laws for Simpson Healthcare to Process Customer Personal Data and provide the Services as described in the Agreement. Customer shall promptly notify Simpson Healthcare and cease Processing Customer Personal Data in the event any required authorization or legal basis for Processing is revoked or terminates.

1. Data Processing.

1.1. Scope and Roles. This DPA applies when Customer Data is processed by Simpson Healthcare. In this context, we will act as processor to Customer, who can act either as controller or processor of Customer Data.

1.2. Customer Controls. Customer can submit requests through the Data Subject Access Rights (DSAR) Portal noted in our Privacy Policy so submit requests related to the Customer's obligations under the GDPR, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that Simpson Healthcare would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Simpson Healthcare becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Simpson Healthcare will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by fulfilling requests submitted through our DSAR portal.

1.3. Details of Data Processing.

1.3.1. Subject matter. The subject matter of the data processing under this DPA is Customer Data.

1.3.2. Duration. As between Simpson Healthcare and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3. Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4. Nature of the processing. Software as a Service (SaaS) and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5. Type of Customer Data. Customer Data provided by and or uploaded to the Customer's SaaS tenant.

1.3.6. Categories of data subjects. The data subjects could include Customer's customers, employees, suppliers and End Users.

1.4. Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to i t and binding on it in the performance of this DPA, including the GDPR.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions) constitute Customer's documented instructions regarding Simpson Healthcare's processing of Customer Data ("Documented Instructions"). Simpson Healthcare will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Simpson Healthcare and Customer, including agreement on any additional fees payable by Customer to Simpson Healthcare for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Simpson Healthcare declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely Simpson Healthcare can form an opinion on whether Documented Instructions infringe the GDPR. If Simpson Healthcare forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. **Confidentiality of Customer Data.** Simpson Healthcare will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Simpson Healthcare a demand for Customer Data, Simpson Healthcare will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Simpson Healthcare may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then Simpson Healthcare will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Simpson Healthcare is legally prohibited from doing so.

3.1. Simpson Healthcare will maintain appropriate physical, technical and organizational informational security measures to protect the integrity, security, and confidentiality of all Customer Personal Data against any anticipated threats or hazards, and/or unauthorized access to or use of Customer Personal Data.

3.2. Customer acknowledges that Simpson Healthcare may change the security measures through the adoption of new or enhanced security technologies and authorizes Simpson Healthcare to make such changes provided that they do not diminish the level of protection. Simpson Healthcare shall make information about the most up to date security measures applicable to the Services available to Customer upon request.

4. **Confidentiality Obligations of Simpson Healthcare's Personnel.** Simpson Healthcare restricts its personnel from processing Customer Data without authorization by Simpson Healthcare. Simpson Healthcare imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. **Assistance with Data Subject Requests.** To the extent Customer does not have the ability to independently correct, amend, or delete Customer Personal Data, or block or restrict Processing of Customer Personal Data, then at Customer's written direction and to the extent required by Data Protection Laws, Simpson Healthcare shall comply with any commercially reasonable request by Customer to facilitate such actions. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures, Simpson Healthcare will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to Simpson Healthcare, Simpson Healthcare will promptly forward such request to Customer once Simpson Healthcare has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, Simpson Healthcare to respond to any data subject who makes a request to Simpson Healthcare, to confirm that Simpson Healthcare has forwarded the request to Customer.

6. Security Incident Notification.

6.1. Security Incident. Simpson Healthcare will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

6.2. Simpson Healthcare Assistance. To enable Customer to notify of a Security Incident to supervisory authorities or data subjects (as applicable), Simpson Healthcare will cooperate with and assist Customer by including in the notification under this Section such information about the Security Incident as Simpson Healthcare is able to disclose to Customer, taking into account the nature of the processing, the information available to Simpson Healthcare, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

6.3. Unsuccessful Security Incidents. Customer agrees that:

6.3.1. an unsuccessful Security Incident will not be subject to this Section. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Simpson Healthcare's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

6.3.2. Simpson Healthcare's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Simpson Healthcare of any fault or liability Simpson Healthcare with respect to the Security Incident.

6.4. Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Simpson Healthcare selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information at all times.

7. Audits and Inspections.

7.1. Internal Audits. Upon written request, Simpson Healthcare shall provide, at its own expense, if available, any data security compliance reports or audit reports that assess the effectiveness of Simpson Healthcare's information security program, system(s), internal controls, and procedures relating to the Processing of Customer Personal Data.

7.2. Customer Audits. Upon request, Simpson Healthcare agrees to respond, no more than once per year, to a reasonable information security questionnaire concerning security practices specific to the Services provided hereunder. Upon reasonable advance written notice in no case fewer than five (30) business days and Simpson Healthcare acceptance, Customer may, not more than once per year, during normal business hours and at its own expense, inspect Simpson Healthcare facilities, networks and procedures directly related to the processing of Customer Personal Data in order to determine compliance with this Agreement. Simpson Healthcare shall reasonably cooperate with such audit by providing access to knowledgeable personnel, physical premises as applicable, documentation, infrastructure, and any application software that Processes Customer Personal Data. Customer shall be responsible for its costs and expenses of such audit. Customer acknowledges that certain information about Simpson Healthcare' security standards and practices are sensitive confidential information which will not be disclosed by Simpson Healthcare to Customer.

7.3. Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the processing and the information available to Simpson Healthcare, Simpson Healthcare will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation.

8. International Transfers

8.1. Simpson Healthcare may Process Customer Personal Data in the United States and anywhere else in the world where Simpson Healthcare or its Sub-processors maintain data Processing operations. Simpson Healthcare shall at all times provide an adequate level of protection for Customer Personal Data, in accordance with the requirements of Data Protection Laws.

8.2. To the extent performance of the Services requires the transfer of Customer Personal Data from within the European Union, the European Economic Area and their member states, Switzerland, or the United Kingdom to a country not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the GDPR), the Standard Contractual Clauses will apply to the transfer and are incorporated by reference herein.

9. **Termination of the DPA**. This DPA will continue in force until the termination of the Agreement (the "Termination Date").

10. **Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, Simpson Healthcare will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion.

11. **Sub-processing.**

11.1. Authorized Sub-processors. Customer provides general authorization to Simpson Healthcare's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("Sub-processors") in accordance with this Section. The Simpson Healthcare lists of Sub-processors that are currently engaged by Simpson Healthcare listed within Annex 1 of this agreement. At least 30 days before Simpson Healthcare engages a Sub-processor, Simpson Healthcare will update Annex 1 and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; or (ii) cease using the Service for which Simpson Healthcare has engaged the Sub-processor.

11.2. Sub-processor Obligations. Where Simpson Healthcare authorizes a Sub-processor:

11.2.1. Simpson Healthcare will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and Simpson Healthcare will prohibit the Sub-processor from accessing Customer Data for any other purpose;

11.2.2. Simpson Healthcare will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by Simpson Healthcare under this DPA, Simpson Healthcare will impose on the Sub-processor the same contractual obligations that Simpson Healthcare has under this DPA; and

11.2.3. Simpson Healthcare will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Simpson Healthcare to breach any of Simpson Healthcare's obligations under this DPA.

12. **Requests, Demands, And Inquiries from Governmental Or Regulatory Bodies.**

12.1. Unless prohibited to do so by applicable law, Simpson Healthcare shall inform Customer as soon as possible if it receives a request or demand from a governmental or regulatory body with authority over Simpson Healthcare or Customer relating to Simpson Healthcare's Processing of Customer Personal Data. Simpson Healthcare may attempt to redirect the government or regulatory body to request that data directly from Customer. As part of this effort, Simpson Healthcare may provide Customer's basic contact information to the government or regulatory body. If compelled to disclose Customer Personal Data to a government or regulatory authority, then Simpson Healthcare shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Simpson Healthcare is legally prohibited from doing so.

12.2. Simpson Healthcare shall provide commercially reasonable cooperation to assist Customer in its response to any requests from a Supervisory Authority relating to the Processing of Customer Personal Data under the Agreement and this DPA.

12.3. Authority in the performance of its tasks relating to this Section, to the extent required under any Data Protection Laws.

13. MISCELLANEOUS.

13.1. Termination and Survival. This Agreement and all provisions herein shall survive so long as, and to the extent that, Simpson Healthcare Processes or retains Customer Personal Data.

13.2. Counterparts. This Agreement may be executed in any number of counterparts and any Party (including any duly authorized representative of a Party) may enter into this Agreement by executing a counterpart.

13.3. Ineffective clause. If individual provisions of this Agreement are or become ineffective, the effectiveness of the remaining provisions shall not be affected. The Parties shall replace the ineffective clause with a legally allowed clause, which will accomplish the intended commercial intention as closely as possible.

Signed for and on behalf of:

Simpson Healthcare

Signature: 

Name: SCOTT ALGIERE

Title: CEO

Date: 10/31/2022

[Customer]

Signature:

Name:

Title:

Date:

Annex 1 - List of Subprocessors

As of the date of this agreement, Simpson Healthcare engages the following Subprocessors that may process Personal Data:

Subprocessor (entity name)	Address	Provided Service
Amazon Web services (AWS)	Primary Region (US East 1) and Secondary Region (US West 2)	Infrastructure as a Service and Platform as a Service
Basecamp	United States	Project Managment service and File Storage
Microsoft Office 365	United States	Email Provider and Office products
Adobe	United States	PDF Reader and Creative Cloud applications
Sage Intacct	United States	Accounting software

Annex 2 - Information Security Measures

Security Program. Simpson Healthcare has developed, implemented, and will consistently update and maintain as needed: (i) a written and comprehensive information security program in compliance with applicable Data Protection Law; and (ii) reasonable policies and procedures designed to detect, prevent, and mitigate the risk of data security breaches or identify theft. Simpson Healthcare will maintain appropriate measures to protect the integrity, security and confidentiality of all Customer Personal Data against any anticipated threats or hazards, and/or unauthorized access to or use of such data, which measures shall include the following:

In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Customer Personal Data;

the encryption of Personal Data;

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;

measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Customer;

Access. Simpson Healthcare shall reasonably update all access rights based on personnel or computer system changes, and shall periodically review all access rights at an appropriate frequency to ensure current access rights to Customer Personal Data are appropriate and no greater than are required for an individual to perform his or her functions necessary to fulfill the purposes of the Agreement. Access controls include:

Changes. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Simpson Healthcare will therefore evaluate the measures as on a periodic basis and will take reasonable measures to maintain compliance with

the requirements. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

Where an amendment to the Service Agreement is necessary in order to execute a Customer instruction to the Simpson Healthcare to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the underlying agreement in good faith.

Physical Security Measures. Simpson Healthcare shall maintain appropriate physical security measures for any facility used to Process Customer Personal Data and continually monitor any changes to the physical infrastructure, business, and known threats.

Simpson Healthcare maintains physical security standards designed to prohibit unauthorized physical access to Simpson Healthcare facilities and equipment by using the following practices:

(0) physical access to locations is limited to Simpson Healthcare employees, subcontractors, and authorized visitors;

(1) Simpson Healthcare employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on premises;

(2) monitoring access to Simpson Healthcare facilities, including restricted areas and equipment within facilities;

(3) access to the data center where Customer Personal Data is hosted is logged, monitored, and tracked; and

(4) data centers are secured with alarm systems and video cameras.

(0) Technical Security Measures. Simpson Healthcare shall:

(0) Perform vulnerability scanning on key applications and infrastructure

(1) Identify computer systems and applications that warrant security event monitoring

(2) Encrypt Personal Data in transit, and where needed, at rest.

(3) Deploy necessary system security patches to all software and systems that process or store Personal Data.

(4) Use up-to-date commercial virus/malware scanning software that identifies malicious code on all of its systems that collect, use, disclose, store, retain or otherwise Process Personal Data.

(5) Use an up-to-date multi-factor authentication solution to ensure that only authorized personnel have access to Customer Personal Data.

(6) Computers and servers have reasonable up-to-date versions of system security software which may include host firewall, anti-virus protection, and up-to-date patches and virus definitions.

(7) Simpson Healthcare maintains logs of various components of the infrastructure and an intrusion detection system.