Equisolve, Inc.
DATA PROTECTION ADDENDUM

This Data Protection Addendum, together with Schedule A and Schedule B (collectively, this "**Addendum**"), shall apply if and to the extent Vendor collects or otherwise processes Customer Personal Data as a processor in connection with the performance of its obligations under the Agreement (each term as defined below). Customer and Vendor are, each, a "**Party**" and, collectively, the "**Parties**". This Addendum is hereby incorporated into, and forms part of, the Agreement.

1. Definitions and Interpretation

1.1 "**Affiliate**" means any entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, a Party. Under this definition of "Affiliate," "**control**" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract, or otherwise.

1.2 "**Agreement**" means (i) Vendor's Terms of Service as entered into between the Parties or (ii) if the Parties have not entered into Vendor's Terms of Service, any other agreement between the Parties that governs the Services.

1.3 "**Business Purpose**" has the meaning given to it in the CCPA.

1.4 "**CCPA**" means the California Consumer Privacy Act of 2018 and any effective regulations relating thereto (for the avoidance of doubt, including as each are amended pursuant to the California Privacy Rights Act).

1.5 "**Customer**" means the Party that entered into the Agreement that is not Vendor.

1.6 "**Customer Personal Data**" means any personal data in respect of which Customer or a Customer Affiliate is a controller or another entity's processor that is processed by Vendor as a processor or subprocessor, respectively, in connection with Vendor's performance of the Services.

1.7 "**DPF**" means, collectively, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework.

1.8 "**EEA**" means, collectively, (a) the then-current member states of the European Union and European Economic Area, respectively, (b) Switzerland, and (c) the United Kingdom.

1.9 "**GDPR**" means, as applicable, (a) the General Data Protection Regulation 2016/679 and all EEA implementation legislation relating thereto, (b) the Swiss Federal Data Protection Act, and (c) the United Kingdom's Data Protection Act 2018 and any transposition of the General Data Protection Regulation 2016/679 into the United Kingdom's domestic law.

1.10 "**Sell**" has the meaning given to it in the U.S. State Privacy Laws.

1.11 "**Services**" means the services and products provided by Vendor to Customer under the Agreement.

1.12 "**Share**" has the meaning given to it in the CCPA.

1.13 "**U.S. State Privacy Laws**" means, as applicable, the CCPA, Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, and any similar United States state privacy laws that provide privacy protections to individuals generally (as opposed to sector-specific laws such as HIPAA, GLBA, Washington My Health My Data Act, Nevada SB370, or children's online safety laws).

1.14 "**Vendor**" means Equisolve, Inc.

1.15 Terms defined in the Agreement shall have the same meaning when used in this Addendum, unless defined in this Addendum. The terms "**controller**," "**data subject**," "**personal data**," "**processing**" (including "**process**" or "**processed**"), "**processor**," and "**supervisory authority**" shall have the meaning defined in, and subject to the territorial and material scope of, the GDPR when used in this Addendum. In cases where applicable privacy laws use the same or different terms to cover concepts similar to those covered under the aforementioned bolded terms (e.g., 'business' instead of "controller," 'consumer' instead of "data subject," 'personal information' instead of "personal data," and 'service provider' instead of "processor"), then "**controller**," "**data subject**," "**personal data**," "**processing**" (including "**process**" or "**processed**"), "**processor**," and "**supervisory authority**" shall have the meaning assigned to those same or different terms under such applicable privacy laws (and shall be subject to the territorial and material scope of such applicable privacy laws).

2. Nature of the Processing

The data processing activities carried out by Vendor as a processor of Customer Personal Data are described in Schedule A to this Addendum.

3. Processor Obligations

(a) Customer and Vendor acknowledge and agree that Customer (or a Customer Affiliate that is authorized to instruct Vendor) is the controller of Customer Personal Data and Vendor is the processor of Customer Personal Data. In certain instances, Customer (or a Customer Affiliate that is authorized to instruct Vendor) may be the processor of Customer Personal Data, in which case Vendor is appointed as a subprocessor of Customer Personal Data. Whether Vendor is serving as a processor or subprocessor of Customer Personal Data, Vendor's obligations regarding the processing of Customer Personal Data shall remain identical and align with Vendor's obligations as a processor pursuant to this Addendum.

(b) Vendor shall only use, disclose, or otherwise process Customer Personal Data (including transfers to third countries from the EEA pursuant to GDPR data transfer obligations) on behalf of and in accordance with Customer's documented, lawful instructions, unless otherwise required or permitted under applicable law. For the avoidance of doubt, the Customer's documented instructions include the provisions of the Agreement.

(c) Customer warrants that Customer discloses Customer Personal Data to Vendor for the Business Purpose of Vendor performing Services for Customer (which, for purposes of the CCPA, aligns with Section 1798.140(e)(5) of the CCPA). Additional details regarding Vendor's Processing of Customer Personal Data are set forth in Schedule A. Vendor shall not Sell or Share Customer

Personal Data. Except as permitted under applicable privacy laws, Vendor shall not retain, use, or disclose Customer Personal Data (i) for any purpose (including, with respect to the CCPA, any "commercial purpose," as such term is defined under the CCPA) other than for the specific purpose of performing the Services or (ii) outside of the direct business relationship between Customer and Vendor. With respect to the CCPA, Vendor shall not combine Customer Personal Data with personal data that Vendor receives from or on behalf of another person (as such term "person" is defined under the CCPA) or that Vendor collects from Vendor's own interaction with data subjects, except as otherwise permitted under the CCPA. Further, Customer's right to take reasonable and appropriate steps to ensure that Vendor processes Customer Personal Data in a manner consistent with Customer's obligations under the CCPA, or to audit Vendor in relation to Vendor's compliance with Vendor's obligations under this Addendum, is as set forth in the **Right to Audit** section of the Agreement.

However, the following is not subject to the **Right to Audit** section of the Agreement: (a) Customer has the right to request (to the extent such request is reasonable) documentation in relation to Vendor's compliance with its obligations as a processor under the U.S. State Privacy Laws and, in response to such request, Vendor shall provide the documentation that Vendor has prepared for general use across its clients regarding such compliance and (b) with respect to the CCPA, Vendor shall notify Customer after Vendor makes a determination that it can no longer meet its obligations under the CCPA and then, upon such notice by Vendor, Customer has the right to take reasonable and appropriate steps to stop and remediate Vendor's unauthorized processing of Customer Personal Data by notifying Vendor that Customer wants to confer with Vendor regarding such unauthorized processing, after which Customer and Vendor will confer in good faith regarding the steps to be taken to remediate such unauthorized processing (and the timelines for completing such steps).

(d) Customer hereby authorizes Vendor to receive Customer Personal Data within, and onward transfer Customer Personal Data to, any country within or outside the EEA. However, where any transfer of Customer Personal Data is a Restricted Transfer, Customer and Vendor (as applicable with respect to such transfer) shall comply with the GDPR's data transfer obligations related thereto before engaging in such transfer. Vendor is validly self-certified under the DPF and is hereby authorized by Customer to engage in Restricted Transfers pursuant to the DPF, to the extent the DPF is applicable to such Restricted Transfer. Taking into account the nature of the processing, Vendor shall assist Customer in responding to data subjects exercising their rights under the DPF Principles.

"**Restricted Transfer**" means, only to the extent the GDPR applies to Customer Personal Data, a transfer of such Customer Personal Data to a country that is not subject to an adequacy determination by the European Commission (in the case of the the General Data Protection Regulation 2016/679), pursuant to Section 17A of the United Kingdom Data Protection Act 2018 (in the case of the transposition of the General Data Protection Regulation 2016/679 into the United Kingdom's domestic law), or by the Bundesrat (in the case of the Swiss FADP).

(e) The Model Clauses are hereby agreed to between the Parties, incorporated by reference into this Addendum, and populated with the information in Schedule B. The Model Clauses will apply to transfers of Customer Personal Data only where the absence of the application of the Model Clauses would cause either Party to breach the GDPR's data transfer obligations. If a relevant

government body deems the Model Clauses and DPF to be inapplicable or invalid data transfer mechanisms under the GDPR, the Parties shall cooperate in good faith to propose and comply with an alternative data transfer mechanism or derogation that is otherwise applicable and valid under the GDPR.

"**Model Clauses**" means (a) (i) Module Two (*controller to processor*) of the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 and (ii) where Customer is serving as a processor under this Addendum on behalf of another entity, Module Three (*processor to processor*) of the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 (collectively, the "**EEA SCCs**"); (b) the mandatory clauses set forth in Part 2 of the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the UK Information Commissioner, together with any other necessary conforming changes to the EEA SCCs (the "**UK SCCs**"); and (c) any updated, revised, or separate clauses relating to applicable data transfer requirements of the GDPR issued from time to time by the European Commission, UK Information Commissioner's Office, any other applicable data protection authority, or other body with competent authority and jurisdiction, together with all necessary conforming changes.

(f) To the extent Customer and Vendor rely on the Model Clauses for the data transfer obligations set forth under Section 3(e), the Parties agree that:

(1) Any provisions excluding or limiting either Party's liability under the Agreement applies to each Party's liability to the other Party under the Model Clauses;

(2) Customer hereby gives Vendor general authorization to engage Subprocessors from an agreed list in accordance with Option 2 of clause 9 of the Model Clauses, and corresponding provisions in relation to Subprocessors (including such list of Subprocessors) are set out in Section 3(j) and Section 3(k) of the body of this Addendum;

(3) The optional language within clause 7 of the Model Clauses does not apply;

(4) The optional language within clause 11(a) of the Model Clauses does not apply;

(5) Clause 17 (Option 1) of the Model Clauses applies and, pursuant to that Option 1 of clause 17, the EEA SCCs will be governed by the laws of Ireland or, in the case of the UK SCCs, the laws of England and Wales will govern (or, where the FADP applies, the laws of Switzerland will govern);

(6) Pursuant to clause 18(b) of the Model Clauses, the Parties shall resolve disputes under the EEA SCCs before the courts of Ireland or, in the case of the UK SCCs, the courts of England and Wales (or, where the FADP applies, the laws of Switzerland will govern);

(7) Table 4 referenced in Part 2 of the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner is not applicable to either Party; and

(8) With respect to transfers covered under the Swiss Federal Act on Data Protection (FADP), (1) the Swiss Federal Data Protection and Information Commission will act as the

competent authority with respect to such transfers and (2) the Model Clauses will apply also with respect to such transfers of data relating to identified or identifiable legal entities until the FADP no longer applies to such entities.

(g) Vendor shall ensure that its personnel authorized to process Customer Personal Data are (i) subject to a duty of confidentiality by contract or (ii) under an appropriate statutory obligation of confidentiality, in each case, with respect to Customer Personal Data.

(h) Vendor shall implement appropriate technical and organizational measures with respect to the Customer Personal Data, after taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, for the purpose of ensuring a level of security appropriate to the risk. A summary of Vendor's security measures is found within this page: https://www.equisolve.com/about/trust-assurance.

(i) Upon becoming aware of an unlawful destruction, loss, alteration, unauthorized disclosure or access of Customer Personal Data or where Vendor otherwise has breach notification obligations to Customer in relation to Customer Personal Data under applicable privacy laws (each, a "**Security Incident**"), Vendor shall notify Customer without undue delay. Taking into account the nature of the processing and the information available to Vendor, Vendor shall provide reasonable details concerning the Security Incident to assist Customer in fulfilling Customer's breach notification obligations under applicable privacy laws. Without prejudice to Vendor's obligations herein, Customer is solely responsible for complying with breach notification laws applicable to Customer and fulfilling any notification obligations to third parties pursuant to any Security Incident.

(j) Subject to the objection right described within this Section 3(j) and solely to the extent authorization of Subprocessors (as such term is defined herein) is required under applicable privacy laws, Customer hereby consents to Vendor's use of Vendor Affiliates and third-party subprocessors ("**Subprocessors**") to process Customer Personal Data pursuant to the Agreement. Vendor will maintain and make available to Customer an up-to-date list of Subprocessors at https://www.equisolve.com/gdpr/dpa/sub-processors, and Vendor will be deemed to have given notice to Customer of an additional or replacement Subprocessor by updating the list ten (10) calendar days prior to such additional or replacement Subprocessor processing Customer Personal Data. Customer may sign up to receive such notice to an email address by designating such recipient email address using the above link. If Customer reasonably objects in writing to an additional or replacement Subprocessor within ten (10) calendar days after notice is given by Vendor in the manner described above regarding such additional or replacement Subprocessor and the Parties cannot resolve Customer's reasonable objection within fourteen (14) calendar days after Vendor's receipt of such reasonable objection, then Customer may terminate the Services impacted by such additional or replacement Subprocessor on written notice to Vendor without penalty and receive a pro-rata refund of any fees paid in advance for the affected Services to which such Subprocessor relates. Where Vendor does not receive a reasonable objection in the manner described in this Section 3(j) or where the Parties have either mutually satisfied concerns of an additional or replacement Subprocessor or Customer has not terminated the Services within fourteen (14) calendar days after being unable to resolve such concerns with Vendor, that additional or replacement Subprocessor shall be deemed authorized by Customer.

(k) Notwithstanding Section 3(j), Vendor may add or replace a Subprocessor without prior notice to Customer if, in its sole discretion, such action is necessary to prevent or mitigate risk to the Services, personal data, technology infrastructure, or customers. Vendor shall give notice of the replacement or additional Subprocessor via the link set forth in Section 3(j) as soon as reasonably possible and Customer shall retain the right to object to such replacement or additional Subprocessor; the timescales for such objection and for resolving any such objection, as set forth in Section 3(j), shall apply to Customer's right of objection in this Section 3(k).

(l) Vendor shall enter into written contracts with its Subprocessors that have substantially similar data protection obligations as those set forth in this Addendum. Where a Subprocessor's act, error, or omission under the aforementioned written contracts results in a breach of this Addendum, Vendor shall remain liable to Customer for that breach of this Addendum up to the extent of Vendor's liability to Customer as set forth under the Agreement.

(m) Taking into account the nature of the processing, and to the extent Customer cannot fulfill such obligations directly via the Services, Vendor shall provide commercially reasonable assistance, including through appropriate technical or organizational measures, insofar as this is possible, to Customer to fulfill its obligations under applicable privacy laws to respond to data subject rights requests and Customer shall provide the information necessary for Vendor to comply with such request. If Vendor receives a request directly from a data subject, Vendor will notify Customer of the request (and, in such notice, Vendor shall include all relevant details provided by data subject) and await Customer's instructions. Notwithstanding the immediately preceding sentence, Vendor may respond to a data subject to the extent required to confirm that such request relates to Customer.

(n) Unless such notification is prohibited under applicable law, Vendor shall promptly notify Customer if a supervisory authority, law enforcement authority, or other regulatory body makes an inquiry regarding, or request for disclosure of, Customer Personal Data, to the extent such inquiry or request expressly names Customer within such inquiry or request.

(o) Upon Customer's request, Vendor shall provide Customer with reasonable assistance with Customer's data protection impact assessment regarding the Services pursuant to the GDPR or U.S. State Privacy Laws by Vendor providing information to Customer regarding the Services that is reasonably necessary for (i) Customer to conduct such data protection impact assessment or (ii) with respect to the GDPR, Customer's prior consultation with a supervisory authority regarding such data protection impact assessment.

(p) Upon termination or expiration of the Agreement, and notwithstanding anything to the contrary in the Agreement, Vendor shall delete all relevant Customer Personal Data (and export a copy of Customer's contact list, as applicable) in Vendor's possession, on the condition that such Customer Personal Data has been sent to Vendor pursuant to Vendor's secure data transfer protocol. Notwithstanding the immediately preceding sentence, where (i) incremental Customer Personal Data is retained in accordance with Vendor's backup procedure or (ii) Vendor is required under any applicable law to retain some or all of such Customer Personal Data (or as may be needed for the establishment, exercise, or defense of legal claims), Vendor shall continue to process such Customer Personal Data after termination or expiration of the Agreement solely to the extent set forth within (i) or (ii), as applicable.

4. General Provisions

(a) Subject to Section 4(b), each Party represents and warrants to the other Party that its performance of its obligations under the Agreement complies with its obligations under the GDPR, CCPA, and all other applicable privacy laws. Further, with respect to the CCPA, Vendor shall provide the same level of privacy protection as is required of "businesses" under the CCPA (as such term "business" is defined under the CCPA) by complying with this Addendum.

(b) Customer represents and warrants that Customer has all required consents (or otherwise have other valid legal grounds or bases), that all required notices or disclosures have been provided, and that Customer otherwise fulfills all legal obligations under applicable law (including any authorizations required from any controllers, where Customer is serving as a processor of another entity) to process Customer Personal Data lawfully, give lawful instruction to Vendor regarding the processing of Customer Personal Data (including instructions given through the Services), and ensure the unencumbered right of Vendor to process Customer Personal Data.

(c) No provision or breach of a provision of this Addendum shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived. Waiver by either Party of a breach of any provision of this Addendum will not operate as a waiver of any other or subsequent breach.

(d) The headings of any sections, subsections, and paragraphs of this Addendum are inserted for convenient reference only and are not intended to be part of or to affect the meaning or interpretation of this Addendum.

(e) Any claims brought under or in connection with this Addendum shall be subject to the terms and conditions set forth in the Agreement, including the exclusions and limitations set forth therein.

(f) The words "include," "includes," or "including" in this Addendum mean, in each case, "including without limiting the generality of the foregoing."

(g) Except to the extent amended by this Addendum, the Agreement remains in full force and effect. If there is a conflict between this Addendum and the Agreement, this Addendum will control to the extent of such conflict. If there is any conflict between the Model Clauses and the rest of this Addendum, the Model Clauses will control to the extent of such conflict. If there is any conflict between an applicable privacy law and this Addendum, the applicable privacy law will control to the extent of such conflict.

Schedule A
Description of Data Processing

The data processing activities carried out by the Vendor under the Agreement may be described as follows:

1. **Subject matter**
   The subject matter concerns the processing of Customer Personal Data pursuant to the Services.

2. **Duration**
   Vendor will process and retain the Customer Personal Data during the term of the Agreement (i.e., on a continuous basis) until instructed otherwise by Customer in accordance with the Agreement.

3. **Nature and purpose**
   Vendor will process Customer Personal Data as necessary to perform the Services and as further instructed by Customer in its use of the Services or through other documentation, as applicable.

4. **Data subjects**
   Vendor shall process the following categories of data subjects:
   - Individuals who visit the Customer website or otherwise use ancillary Services, including web/tele-conferencing;
   - Individuals who subscribe to email alerts on Customer website;
   - Individuals who submit a form on Customer website; and
   - Authorized Users

5. **Personal data categories**
   Processing concerns the following categories of Customer Personal Data:
   - Customer prospective or current investor or website visitor contact or business information including name, email address, phone number, and any other personal data processed through Customer website or otherwise via the Services;
   - Authorized User log-in information (e.g., username, password);
   - Technical information including IP address, browser user agent string, and any other information required to provide the Services or related to the use of cookies, pixel tags, and similar technologies for analytics, chat, marketing, or advertising purposes directed by Customer; and
   - Other data categories as instructed by Customer to be processed by Vendor.

6. **Processing Operations**: The Services contemplated under the Agreement; in general, maintenance of website and related content management system, including sending of emails and embedding of scripts as directed by Customer and provision of log-in credentials, provision of webconferencing and similar services, and other operations as directed by Customer.

7. **Special categories of personal data/sensitive personal data**: N/A

Schedule B
Model Clauses

Information deemed incorporated into the Model Clauses	
Data exporter	**Name of the data exporting organization**: Customer Customer company information listed in the Agreement (or related Purchase Order Agreement) is incorporated by reference herein.
Data importer	**Name of the data importing organization**: Vendor Vendor company information listed in the Agreement (or related Purchase Order Agreement) is incorporated by reference herein.
Annex I.A	**List of Parties**: Relevant information regarding "Data exporter" and "Data importer" under this Schedule B are incorporated by reference herein.
Annex I.B	**Description of Transfer**: Relevant information from Schedule A above is incorporated by reference herein. The subject matter and nature of processing by Sub-processors is as set forth here (https://www.equisolve.com/gdpr/dpa/sub-processors) under "Purpose" and is also as aligned with the subject matter and nature set forth in Schedule A. The duration of processing is aligned with the duration set forth in Schedule A.
Annex I.C	**Competent Supervisory Authority**: The competent supervisory authority shall be determined based on the situation applicable to the data exporter under clause 13 of the Model Clauses (e.g., if the data exporter is established in an EU member state, or falls under GDPR Article 3(2) and has an appointed representative under GDPR Article 27(1), or falls under GDPR Article 3(2) and has not appointed a representative under GDPR Article 27(1)), *except that*, (i) in the case of the UK SCCs, the competent supervisory authority under the UK SCCs will be the United Kingdom Information Commissioner and (ii) with respect to transfers covered under the Swiss FADP, the Swiss Federal Data Protection and Information Commission will act as the competent authority with respect to such transfers.
Annex II	**Technical and Organisational Measures**: https://www.equisolve.com/about/trust-assurance