DATA PROCESSING ADDENDUM TO AGILLINK USER AGREEMENT

Last Modified: March 18, 2024

This Data Processing Addendum (this "**Addendum**") reflects the parties' agreement with respect to the Processing of Personal Data by Datafaction, Inc., d/b/a AgilLink ("**AgilLink**") on behalf of Customer in connection with the Services provided by AgilLink to Customer pursuant to that certain Agreement between AgilLink and the Customer.

1. Definitions. The following terms shall have the meaning ascribed below. Capitalized terms not defined herein or in the Agreement such as "Business Purpose," "Financial Institution," "Process," and "Sale" shall have the meaning set forth in applicable Data Protection Laws and, where terms are defined in the Agreement, they shall have the meaning set forth therein.

"**Affiliate**" means any entity controlling, controlled by, or under common control with the referenced entity, where the term "control" means the possession, direct or indirect, 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.

"**Agreement**" means that certain Agreement whereby AgilLink provides access to the Services to Customer.

"**Customer**" means the company or other legal entity that is party to the Agreement.

"**Consumer**" means an identified or identifiable person or household and includes a "data subject" as defined in the Data Protection Laws and a "customer" as defined in the Gramm-Leach-Bliley Act ("**GLBA**").

"**Consumer Data**" means any and all information provided to the parties by Consumers, as well as information collected by the parties concerning Consumers' use of the Services.

"**Controller**" means the party that determines the purposes and means of the Processing of Personal Data and includes a "Business" as defined in the CCPA.

"**Data Protection Laws**" means laws, regulations, or guidance applicable to the Processing of Personal Data pursuant to the Agreement, including the GLBA, GDPR, the California Consumer Privacy Act ("CCPA"), the New York Cybersecurity Regulation (23 NYCRR 500).

"GDPR" means Regulation (EU) 2016/679 of The European Parliament and The Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of those data and repealing Directive 95/46 / EC (General Data Protection Regulation).

"**Personal Data**" means any information relating to a Consumer that is Processed by AgilLink on behalf of Customer and includes all "personal information," "nonpublic personal information," "personally identifiable information," "personal data" or similar terms as defined by Data Protection Laws.

"**Processor**" means the party which Processes Personal Data on behalf of the Controller and also means a "service provider" as defined in the GLBA and CCPA.

"**Safeguards**" means the physical, technical, organizational, and administrative controls designed to ensure the security and confidentiality of Customer's Personal Data, which shall contain appropriate and adequate security measures, procedures and practices sufficient to protect the Customer's Personal Data against any reasonably anticipated risks.

"**Security Incident**" means any known unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Customer's Personal Data or any known compromise of any system that contains or Processes Customer's Personal Data.

"**Security Standards**" means applicable legal, regulatory, industry, business, and/or contractual guidelines, policies, and/or requirements relating to the protection, safeguarding, and/or security of Personal Data.

"**Services**" means the specialized accounting software-as-a-service products (or similar services) made available by AgilLink to which Customer subscribes and has access under the Agreement, which products or services are more specifically described Agreement.

"**Subprocessor**" means any person, or subcontractor appointed by or on behalf of a Processor to Process Personal Data on behalf of a Controller.

"**WISP**" means a written information security program that contains a party's Safeguards and meets the requirements to maintain an information security program under any Applicable Law.

2. Business Purpose. In providing the Services, AgilLink will Process Personal Data on behalf of Customer, which acts as a Controller with respect to such Personal Data. AgilLink will Process Personal Data for the purposes set forth in the Agreement and/or such other purposes as are specified in documented instructions provided by Customer.

3. AgilLink's Role and Responsibilities. AgilLink agrees and acknowledges that it is a Processor and understands its obligations as a Processor under applicable Data Protection Laws. Accordingly, AgilLink shall only Process Personal Data as set forth below:

(a) AgilLink shall comply with Data Protection Laws when Processing Personal Data.

(b) AgilLink shall only Process Personal Data on documented instructions from Customer and solely to fulfill the Business Purpose, including with regard to transfers of Personal Data to a third country or to an international organization, and solely in such manner as is necessary for the provision of the Services under the Agreement**.**

(c) AgilLink shall provide Customer with all reasonably requested assistance and cooperation to enable Customer to comply with and fulfill its obligations under applicable Data Protection Laws, including assisting Customer in responding to any Consumer rights requests relating to Personal Data. AgilLink will promptly notify Customer if AgilLink receives a request directly from a Consumer or regulator under any Data Protection Laws and will not respond to such request except on the documented instructions of Customer or as required by Applicable Law.

(d) AgilLink will provide reasonable cooperation and assistance to Customer in conducting any data protection impact assessment required by applicable Data Protection Laws or regulatory authority.

(e) AgilLink is strictly prohibited from retaining, using, and/or disclosing Personal Data for any reason or purpose other than fulfilling the Business Purpose and shall not disclose use and/or disclose Personal Data in any way that could be construed as a Sale of Personal Data under Data Protection Laws or in any way not permitted for Processors.

(f) Unless necessary to provide the Services or otherwise specified in the Agreement, AgilLink is prohibited from combining Personal Data received from Customer with Personal Data from other sources, including that which AgilLink collects on its own interaction with the Consumer.

(g) AgilLink will retain Personal Data only as directed by Customer or as required by Applicable Laws. At the termination of the Agreement, or upon Customer's written request, AgilLink will either, at Customer's option, destroy or where commercially reasonable return to Customer and destroy all copies of Customer's Personal Data and certify to the destruction thereof, unless and to the extent legal obligations require storage of Personal Data. Such data destruction shall conform to the FTC's regulation governing disposal of consumer information and records disposal (16 CFR 682), as well as any Data Protection Laws. In the event AgilLink retains any Personal Data, AgilLink shall not access or utilize such retained data following termination of this Addendum or the Agreement, and AgilLink shall secure and retain such records in accordance with AgilLink's retention policies and/or schedules.

(h) AgilLink will treat all Personal Data as Customer's Confidential Information and will not disclose Personal Data to third parties except as permitted by this Addendum or the Agreement.

(i) AgilLink shall promptly notify Customer if AgilLink is unable to comply with its duties under any applicable Data Protection Laws and will, in such case, cease further Processing of data on Customer's behalf. Without limiting the foregoing, AgilLink shall, upon Customer's or its designee's request, cooperate in good faith with Customer to enter into additional or modified terms to address any modifications, amendments or updates to any applicable Data Protection Laws.

4. Safeguards. AgilLink shall implement and maintain at all times reasonable and appropriate Safeguards designed to ensure the integrity, security, and confidentiality of Customer Personal Data. Such Safeguards shall: (i) comply with all applicable Data Protection Laws; (ii) reasonably protect Customer's Consumer Personal Data against Security Incidents; and (iii) meet or exceed applicable Security Standards as well as any security requirements set forth in any Applicable Law. Upon request, AgilLink shall provide to Customer the information, documents and materials reasonably necessary to evidence such Safeguards.

(a) Written Information Security Program. AgilLink will maintain a comprehensive WISP designed and implemented with administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of Personal Data, including Personal Data. The WISP shall have documented policies, standards, and procedures designed to ensure that all such Safeguards, including the manner in which Personal Data is collected, accessed, used, stored, processed, disposed of, and disclosed, are clearly defined, developed, and implemented to manage risks to information assets.

(b) Access Controls. AgilLink shall implement and periodically review its access controls, including technical and physical controls to: (i) authenticate and permit access only to authorized personnel to protect against the unauthorized acquisition of Personal Data; (ii) limit authorized personnel access only to Customer Personal Data that they need to perform their duties and functions; and (iii) immediately terminate access to Personal Data when a person no longer qualifies as authorized personnel.

(c) Network Security. AgilLink shall maintain reasonably appropriate firewalls and access control lists between all AgilLink and Customer networks, with only required traffic allowed between networks.

5. Subprocessors. AgilLink shall not engage any Subprocessors for the performance of any part of the Services without notifying Customer. To the extent such a Subprocessor is so engaged and is or will be provided with Customer's Personal Data in connection with its performance of the Services, AgilLink will conduct appropriate due diligence on such Subprocessor to confirm that such Subprocessor can comply with the requirements of this Addendum. AgilLink will bind each such Subprocessor by written contract to obligations substantially similar to those owed by AgilLink to Customer under the Agreement and this Addendum. AgilLink has currently engaged, as Subprocessors, the third parties listed on https://www.agillink.com/content/dam/agillink/privacy-and-disclosures/**subprocessor**.pdf to assist AgilLink in the performance of the Services.

6. Audit Rights. Upon fifteen (15) business days notice and during regular business hours, Customer may audit AgilLink's compliance with this Addendum, including AgilLink's Safeguards. AgilLink shall reasonably cooperate with any such audit and, upon Customer's prior written request, furnish evidence, to the extent available, of compliance.

7. Security Incidents. AgilLink shall notify Customer of any Security Incident, within seventy two (72) hours following AgilLink's confirmation of any such Security Incident.

8. Term. The term of this Addendum shall begin upon the Effective Date and shall continue in full force and effect until the terimination of all Services under the Agreement. This Addendum shall otherwise remain in full force and effect through the completion or earlier termination of the Services.

9. General Provisions.

(a) **Amendments and Modifications.** Notwithstanding anything else to the contrary in the Agreement, AgilLink reserves the right to make any updates and modifications to this Addendum at any time and at its sole discretion.

(b) **Severability.** If any individual provisions of this Addendum are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this Addendum will not be affected.

(c) **Limitation of Liability.** Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this Addendum (and any other Addenda between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Damages' section of the Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this Addendum). Notwithstanding the foregoing, in no event will either party's liability be limited with respect to any individual's data protection rights under this Addendum (including the Standard Contractual Clauses) or otherwise to the extent that so limiting liability is or would be prohibited by Applicable Law.

(d) **Conflicts.** In the event of a conflict between the terms of the Agreement and the Addendum, this Addendum shall control.

(e) **Governing Law.** This Addendum will be governed by and construed in accordance with the 'Governing Law; Jurisdiction and Venue' section of the Agreement, unless required otherwise by Data Protection Laws.