DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") to process Personal Data (defined below), is entered into by and between **Legility, LLC and its Affiliates** (collectively, "**Legility**"), and Legility's respective clients (each a "**Client**"), and is entered into in connection with Legility's Services to Client to process Agreement Personal Data (defined below) under an agreement between the parties (the "**Agreement**"); this Addendum forms an integral part of the Agreement and, accordingly, its terms are incorporated into the Agreement by reference.

1. **Definitions and Interpretation**.

1.1 For purposes of this Addendum, the terms set forth below shall mean as follows:

"**Affiliate**" means, with respect to a particular party, an entity that is Controlled by, Controlling, or in common Control with, that party, where "**Control**", "Controlled", "Controlling", and "in common Control with" mean the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting shares, by contract, or otherwise.

"**Agreement Personal Data**" means any Personal Data (including sensitive or special categories of data) that is processed under, or in connection with, the Agreement.

"**Controller"** means the natural or legal person, public authority, agency, or other body that alone or jointly (i.e., with others) determines the purpose(s) and means of Processing the Personal Data.

"**Data Protection Law(s)**" means any applicable data protection laws relating to the protection of individuals with regards to the processing of Personal Data including (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"), (ii) laws implemented by the European Union member states which contain derogations from, or exemptions or authorizations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR, (iii) any legislation that, replaces or converts into domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union; and/or any corresponding or equivalent national laws or regulations including any amendment, update, modification or re-enactment of such laws; (iv) the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq.*, and its implementing regulations ("CCPA"); (v) requirements for service providers set forth in Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth; (vi) the New York Stop Hacks and Improve Electronic Data Security Act ("SHIELD ACT"), N.Y. Gen Bus. Law§ 899-bb; (vii) Japan's Act on the Protection of Personal Information ("APPI"); (viii) Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"); and, (ix) any other similar laws and regulations that prescribe requirements applicable to service providers of Personal Data.

"Data Subject" means a natural person.

"**EU Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to processors established in countries outside the European Union which do not ensure an adequate level of protection as set out in Commission Decision C(2010)593 of 5 February 2010, as updated, amended, replaced, or superseded from time-to-time by the European Commission.

"**Personal Data**" means any data that identifies or, alone or in combination with any other data, could reasonably be used to identify, locate, or contact a natural person or household, or any other information that is considered "personally identifiable information," "personal information," "personal data," or other similar terms under applicable Data Protection Law(s).

"**Personal Data Breach**" means any verified breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Agreement Personal Data.

"**Process**", "**Processing**" or "**Processed**" means any operation or set of operations that are performed upon Personal Data, whether by automatic means, such as collecting, accessing, processing, using recording, organizing, storing, adapting or altering, retrieving, consulting, disclosing, disseminating, transmitting, aligning or combining, blocking, erasing, destroying, or otherwise using in a manner set forth in Data Protection Laws.

"**Processor**" means an entity that processes information only on behalf of the Controller.

"**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, electronically, or by other means, a Data Subject's Personal Data to a third party for monetary or other valuable consideration.

"**Services**" means performance of the services and activities provided pursuant to, or in connection with, the Agreement previously entered into between Legility, and in addition to any other services described in the Agreement for which Legility receives or accesses Agreement Personal Data.

"**Service Provider**" means an entity that processes information on behalf of a business and to whom the business discloses a Data Subject's Personal Data for a business purpose pursuant to a written contract.

"**Subprocessor**" means a Legility processor engaged by Legility to carry out specific processing activities on Agreement Personal Data.

"Supervisory Authority" means any local, national, or multinational agency, department, official, parliament, public, or statutory person, or any other government or professional body, regulatory or supervisory authority, board, or other body responsible for administering applicable Data Protection Laws.

1.2 To the extent the terms contained in this Addendum conflict, or are inconsistent, with terms relating to the same subject matter in the Agreement, the terms contained in this Addendum shall prevail.

1.3 Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. Data Protection Obligations.

2.1 **Role of the Parties**. With respect to the Agreement Personal Data Processed pursuant to the Services Legility provides under the terms of the Agreement, Legility acts as a Processor on behalf of Client, who is a Controller of the Agreement Personal Data.

2.2 **Compliance with Data Protection Laws**. Each party undertakes to comply with all Data Protection Laws applicable to the Processing of Agreement Personal Data and will not knowingly cause the other to breach Data Protection Laws. The parties acknowledge and agree that the description of the Processing and any specific Processing instructions with respect to Personal Data, in addition to those stated in Exhibit B, shall include any relevant descriptions or instructions set forth in the Agreement. In its capacity as a Controller, Client confirms that all Agreement Personal Data that is (i) collected by Client, (ii) sourced by Client, (iii) sourced on Client's behalf, or (iv) otherwise made available to Legility, for Processing in connection with the Services and the performance of the Agreement shall comply, and was collected or otherwise obtained in compliance, with Data Protection Laws, including Client's responsibility to ensure that there is a lawful basis for each Processing activity that Client instructs Legility to perform in relation to the Agreement. As necessary, Client will obtain appropriate individual consents to collect Personal Data before sharing the Personal Data with Legility for Processing.

2.3 **Scope of Processing**. Solely in accordance with applicable Data Protection Laws, Client instructs Legility to Process Agreement Personal Data: (i) to provide the Services; (ii) as further specified via Client's use of the Services, if applicable; (iii) as documented in the Agreement (or any statement of work entered into under the Agreement, if applicable), including this Addendum; and, (iv) as further documented in any other written instructions given by Client, and acknowledged in writing by Legility, as constituting instructions for purposes of this Addendum.

3. **Use of Personal Data**. Legility, as a Service Provider, agrees not to Sell Agreement Personal Data. Legility will not retain, use, or disclose Agreement Personal Data for any purposes other than specified herein, including, without limitation, performing the Services. If Legility is legally required by Data Protection Laws, or other applicable law, to Process Client Personal Data other than as instructed by Client, Legility will notify Client before such Processing occurs, unless the law requiring such Processing prohibits Legility from notifying Client on an important ground of public interest, in which case Legility will notify Client as soon as that law permits Legility to do so. Legility may aggregate, de-identify, or anonymize Personal Data, so that it no longer meets the Personal Data definition, and may use such aggregated, de-identified, or anonymized data for its own research and development purposes. Legility will not attempt to, nor actually re-identify, any previously aggregated, de-identified, or anonymized data.

4. **Security**. Legility shall implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the Processing, and the nature, of the Agreement Personal Data, including, as may be appropriate: (i) pseudonymisation and encryption; (ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services; (iii) the ability to restore the availability and access to the Agreement Personal Data in a timely manner in the event of a physical or technical incident; and, (iv) a process for regulatory testing, assessing, and evaluating the effectiveness of such measures. A description of Legility's security measures is attached hereto as Exhibit C. Without prejudice to Legility's data security obligations under this Addendum, Client is responsible for its use of the Services and its storage of Agreement Personal Data outside of Legility's or Legility's Subprocessors' systems, including: (i) implementing reasonable additional security controls to ensure a level of security appropriate to the risk related to the Agreement Personal Data; (ii) securing the account authentication credentials, systems, and devices that Client uses to access the Services; and, (iii) retaining copies of its Agreement Personal Data, as appropriate.

5. **Legility Employee Confidentiality**. Legility will ensure that personnel who have access to Agreement Personal Data are (i) informed of the confidential nature of the Agreement Personal Data and obliged to keep such Agreement Personal Data confidential, and (ii) aware of Legility's duties and obligations under the Agreement and this Addendum.

6. **Rights of Data Subjects**.

6.1 **Data Subject Requests.** Legility shall promptly notify Client if it receives a request from a Data Subject to exercise the Data Subject's rights under the applicable Data Protection Law ("Data Subject Request"). Taking into account the nature of the Processing of the Agreement Personal Data, Legility will use commercially reasonable and appropriate technical and organizational measures to assist Client with the fulfilment of its legal obligation(s) to respond to the Data Subject

Request. To the extent legally permitted, Client shall be responsible for any costs arising from Legility's provision of such assistance.

6.2 **Personal Data Breach**. Upon becoming aware of any Personal Data Breach, Legility will notify Client without undue delay, and will provide reasonable assistance to Client in response to such Personal Data Breach to enable Client to meet its notification obligations to supervisory authorities and/or affected Data Subjects. under applicable Data Protection Laws For these purposes, and as Client reasonable requires, Legility will provide details (to the extent that such details are known to Legility) regarding: (i) the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects affected; (ii) any investigations into such Personal Data Breach; (iii) the likely consequences of the Personal Data Breach; and, (iv) any measures taken, or that Legility recommends be taken, to address the Personal Data Breach, including to mitigate its possible adverse effects. The parties agree that the details set out under (i) to (iv) above may be provided to Client in phases, as the information becomes known to Legility.

7. **Deletion or Return of Personal Data**. Legility shall return to Client the Agreement Personal Data and, to the extent permitted by applicable law, delete Agreement Personal Data after termination of the Agreement or the expiration of any confidentiality obligations.

8. **Subprocessors**.

8.1 **Consent**. Except with respect to Legility's Subprocessors, who are listed in the attached Exhibit A and are deemed to be approved by Client, Legility will not engage a Subprocessor to undertake any material Processing of Agreement Personal Data, other than as previously disclosed to Client, unless Subprocessor is subject to a written agreement which imposes substantially equivalent obligations on that Subprocessor as are imposed on Legility by Client. Legility will notify Client of its intent to engage a material Subprocessor and, in the event Client objects to such Subprocessor, Client and Legility shall cooperate in good faith to make such adjustments as necessary to satisfy Client's concerns. If, within five (5) days of Legility's Section 8.1 notice (the "Notice Period"), Client has not approved Subprocessor, then Client or Legility shall have the right to terminate the applicable portion of the Agreement, or the applicable purchase order, statement of work, or other ordering document; and, if not so terminated by either party at the end of the Notice Period, Subprocessor shall be deemed approved.

8.2 **Subprocessor Transfer of Personal Data**. Client hereby consents to Legility and its Subprocessors Processing Personal Data in a jurisdiction other than one that the European Commission has found to offer an adequate level of protection for Personal Data provided that: (i) the relevant "data exporter" and "data importer" are bound by the EU Standard Contractual Clauses as related to the Processing of Agreement Personal Data, or (ii) the relevant "data importer" maintains a lawful mechanism approved by the governing regulatory body under the respective Data Protection Law applicable to the transfer of Personal Data.

9. **Audit**.

9.1 **Compliance.** On Client's written request, Legility shall provide Client with information that is reasonably necessary to demonstrate Legility's compliance with its data protection obligations under this Addendum; and, Legility shall permit, and contribute to, audits (including inspections) conducted by Client or an auditor mandated by Client, but only: (i) if such information and audits are in relation to the Agreement Personal Data Processed pursuant to the Agreement; and, (ii) to the extent that such information and audits are required under applicable Data Protection Law.

9.2 **Inspection.** Client agrees that any audit or inspection requested in accordance with Section 9.1 shall be conducted: (i) upon not less than fifteen (15) days' prior written notice, (ii) not more than once per calendar year, (iii) during normal business hours, (iv) causing minimal disruption to Legility's day-to-day business; and, (v) in accordance with Legility's obligations of confidentiality. Legility may charge a fee (based on Legility's reasonable costs) for any audit or inspection performed under this Addendum. Legility will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such audit or inspection. Client will be responsible for any fees charged by any auditor or inspector appointed by Client to execute any such audit or inspection. Legility may object in writing to an auditor or inspector appointed by Client to conduct any audit or inspection under this Addendum if the auditor or inspector is, in Legility's reasonable opinion, not suitably qualified or independent, a competitor of Legility, or otherwise manifestly unsuitable. Any such objection by Legility will require Client to appoint another auditor or inspector or conduct the audit itself.

10. **Limitation of Liability**. The terms and conditions stated in this Addendum, whether related to, or adopted independently of, an existing agreement between Client and Legility, shall at all times be subject to the limitation of liability or similar terms of the Agreement covering the applicable Processing.

11. **Governing Law**. This Addendum is governed by the law of the country that governs the Agreement and the parties submit to the jurisdiction of the courts referred to in the Agreement without regard to provisions related to conflicts of law.

12. **Miscellaneous**. Client may require Legility to accept additional data privacy terms necessary to address applicable data protection, privacy, or security laws. If Legility is unable to agree to such additional data privacy terms, Legility may terminate this Addendum without penalty on thirty (30) days' written notice. Except as amended by this Addendum, all terms and conditions of the Agreement shall remain in full force and effect. Nothing in this Addendum or the Agreement relieves Client of its own direct responsibilities and liabilities under the Data Protection Laws. With respect to the Processing of Agreement Personal Data, if there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

13. **European Specific Provisions**.

13.1 **GDPR**. Legility will Process Agreement Personal Data in accordance with the GDPR requirements directly applicable to Legility's provision of its Services.

13.2 **Data Protection Impact Assessment.** Upon Client's written request, and to the extent(i) Client does not otherwise have access to the relevant information, and (ii) such information is available to Legility, Legility shall provide Client with reasonable assistance needed to fulfill Client's obligation under the GDPR to carry out a data protection impact assessment related to Client's use of the Services. Legility shall provide reasonable assistance to Client in the cooperation, or prior consultation, with the Supervisory Authority in the performance of its tasks to the extent required under the GDPR.

13.3 **Transfer Mechanisms for Data Transfers**. Legility and its Affiliates located in the United States of America shall utilize Standard Contractual Clauses for transfers of Personal Data outside of the European Union and/or their member states, or any other jurisdictions that have similar laws and regulations regarding the transfer of Personal Data. The EU Standard Contractual Clauses ("SCCs") are located at: https://info.legility.com/hubfs/SCCs.pdf, under "Data Security and Protection", and incorporated herein as an integral part of this Agreement.

EXHIBIT A

List of Pre-Approved Subprocessors for Services (if applicable):

A list of Legility's pre-approved Subprocessors may be found at: https://www.legility.com/data-security-and-protection.

EXHIBIT B

DETAILS OF PROCESSING OF PERSONAL DATA

Subject matter and duration of the Processing of Client Personal Data

The subject matter, nature, purpose, and duration of the Processing of the Agreement Personal Data are set out in the Agreement, and may be further stated in this Exhibit B below, or described elsewhere in this Addendum.

Data Subjects

The Agreement Personal Data transferred to Processor is determined and Controlled by Client in its sole discretion.

Categories of Data

The Personal Data transferred to, or accessed by, Processor includes all relevant information required to deliver requested Services under the Agreement, is determined and controlled by Client in its sole discretion, and may include:

- Personal details such as first and last name, email address, telephone number, and/or physical address;
- Authentication credentials to use part of the Services, such as username, IP address, PC name, etc.;
- Activities performed by Controller personnel, its agents, contractors or affiliates as users of the performed services; and,
- Any other category of data agreed upon between the parties in an agreement.

Special Categories of Personal Data (if appropriate)

The Agreement Personal Data may concern the following special categories of data:

- With regard to Clients in the healthcare industry, data governed by specific privacy regulations;
- With regard to Clients in the financial sector and other regulated industries, data covered under specific privacy regulations; and,
- With regard to employment and similar litigation matters, data concerning race, national origin, or gender.

Processing operations

Agreement Personal Data will only be Processed for the purpose of, and to the extent necessary for, the performance of the Services requested from Legility by Client under the Agreement, and will be subject to the basic Processing activities set out in the Agreement for the performance of Services.

EXHIBIT C

LEGILITY DATA SECURITY MEASURES

A description of Legility's security measures can be found at: https://www.legility.com/data-security-and-protection.