DATA PROCESSING ADDENDUM

This Data Processing Addendum and its Exhibits (the "**Addendum**") is made and entered into by and between Centercode, Inc. ("**Centercode**") and the customer specified in the table below ("**Customer**"). The Customer signatory below represents to Centercode that he or she has legal authority to bind Customer and is lawfully able to enter into this Addendum. Each party's signature below constitutes signature of the Addendum and Standard Contractual Clauses and its Appendices.

CENTERCODE, INC., a California corporation	**CUSTOMER NAME:** _______________________________ (full legal entity name)
By: _______________________________	**By (Sign Here):** _______________________________
Name: Luke Freiler	**Name:** _______________________________
Title: Chief Executive Officer	**Title:** _______________________________
Date: _______________________________	**Date:** _______________________________
Address: **23422 Mill Creek Drive, Suite 105** **Laguna Hills, CA 92653** **Attn: CEO**	**Address:** _______________________________ _______________________________ _______________________________ **Attention:** _______________________________

This Addendum includes the Data Processing Terms, Exhibit 1 (Details of Processing), Exhibit 2 (Centercode Security Standards), and where applicable, the Professional Services Exhibit, and supplements, amends, and is incorporated by reference into Customer's Agreement with Centercode. This Addendum will be effective as of the day that Centercode countersigns a complete and executed Addendum from Customer in accordance with the following instructions (the "**Effective Date**").

INSTRUCTIONS

Please (1) complete the table above by signing and providing the customer full legal entity name, address, and signatory information; and (2) submit the complete and signed Addendum to Centercode via email to privacy@centercode.com.

DATA PROCESSING TERMS

1. DEFINITIONS

In this Addendum:

"**Affiliate(s)**" shall have the same meaning as ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by, or under common control with a party, where control means the ownership of a majority share of the stock, equity, or voting interests of such entity.

"**Administrators**" has the definition provided in the Agreement, or if none, it means the Customer's end users of the Services assigned roles by the Customer within the Services that enable the administration of some or all of the Services, including but not limited to "Community Administrators" in the Services.

"**Agreement**" means the agreement between Centercode and Customer that incorporates this Addendum and contains the terms and conditions governing the provision of the Services, and any order forms or order documents entered into under that agreement.

"**Applicable Data Protection Laws**" means legislation, and rules and regulations adopted thereunder, as amended or superseded from time to time, relating to data protection and privacy applicable to the processing of Personal Data in connection with the Services, including applicable United States federal laws, Applicable US State Privacy Laws, and Applicable European Data Protection Laws, in each case where and to the extent applicable.

"Applicable European Data Protection Laws" means data protection and privacy laws in Europe and their implementing regulations, as amended or superseded from time to time, including: (i) the GDPR; (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("**Swiss FDPA**"); and (v) other applicable data protection and privacy laws and regulations of the European Union, the EEA, and their member states, Switzerland, and the United Kingdom, in each case where and to the extent applicable.

"**Applicable US State Privacy Laws**" means U.S. state data protection and privacy laws and their implementing regulations, as amended or superseded from time to time, including but not limited to: (i) the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (the "**CCPA**"); (ii) the Colorado Privacy Act; (iii) the Connecticut Personal Data Privacy and Online Monitoring Act; (iv) Utah Consumer Privacy Act; and (v) Virginia Consumer Data Protection Act, in each case where and to the extent applicable.

"Betabound" means Centercode's web-based portal and community used by Centercode to register third parties interested in participating in product and service tests of Centercode's customers and other third parties and to announce these tests.

"**Betabound Personal Data**" means personal data or information (as defined under Applicable Data Protection Laws) of members of Centercode's Betabound community that is collected from such members into Centercode's Betabound portal (such personal data or information being owned and controlled by Centercode) and that is shared by Centercode with Customer or its Affiliates in connection with the Services.

"**Centercode Platform**" means Centercode's proprietary, cloud-based software-as-a-service platform designed for product and service testing programs (e.g. Beta and Delta testing programs).

"**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data and shall be interpreted in accordance with Applicable Data Protection Laws. For the sake of clarity, as applicable, Controller includes "Business" as defined in Applicable US State Privacy Laws.

"**Customer Data**" means the data submitted or provided by Customer (or its account holders) to its implementation(s) of the Centercode Platform while using the Services (not including Customer Business Contact Data).

"**Data Subject**" means the individual to whom the Personal Data relates and shall be interpreted in accordance with Applicable Data Protection Laws. For the sake of clarity, as applicable, Data Subject includes "Consumer" as defined in Applicable US State Privacy Laws.

"**EEA**" means the European Economic Area.

"**Europe**" means member states of the EEA, the United Kingdom, and Switzerland.

"**European Personal Data**" means Personal Data that is subject to the protection of Applicable European Data Protection Laws.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"**Personal Data**" means any Customer Data that relates to an identified or identifiable individual where the information is protected as personal data or personal information under Applicable Data Protection Laws and shall be interpreted in accordance with Applicable Data Protection Laws. For the sake of clarity, as applicable, Personal Data includes "Personal Information" as defined in Applicable US State Privacy Laws.

"**Processing**" (or "**Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and shall be interpreted in accordance with Applicable Data Protection Laws.

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller and shall be interpreted in accordance with Applicable Data Protection Laws. For the sake of clarity, as applicable, Processor includes "Service Provider" and "Contractor" as defined in Applicable US State Privacy Laws.

"**Professional Services**" has the definition provided in the Agreement and, if not defined in the Agreement, the term means Services provided by Centercode to Customer, other than subscription-based access to the Centercode Platform and/or any Centercode Platform add-ons such as enhancements and additional features, or support.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored, or otherwise Processed by Centercode or its Sub-Processors in connection with the provision of the Services, and does not include unsuccessful activities, attacks, or attempts to access Personal Data that do not compromise the security of the Personal Data.

"**Services**" means those services provided by Centercode to Customer under the Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, currently found at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf, as may be amended, superseded, or replaced.

"**Sub-Processor**" means a third-party engaged by Centercode in connection with Centercode's performance of the Services that Processes Customer's Personal Data. The term Sub-Processor does not include any Centercode personnel, whether employee or independent contractor.

"**Supervisory Authority**" shall be interpreted in accordance with Applicable European Data Protection Laws.

"**UK SCC Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded, or replaced.

2. APPLICABILITY OF THIS ADDENDUM AND TERM

2.1 Applicability. This Addendum shall apply only to the extent: (a) Centercode Processes Personal Data on behalf of Customer in connection with the Services; and/or (b) as applicable, where Centercode shares Betabound Personal Data with Customer in connection with its performance of Professional Services. If and to the extent the Services include the performance by Centercode of Professional Services on Customer's behalf, as documented in a mutually executed Order Form, the Professional Services Exhibit to this Data Processing Addendum applies.

2.2 Term. This Addendum will terminate automatically upon termination of the Agreement except to the extent expressly provided otherwise in this Addendum.

3. ROLES AND RESPONSIBILITIES

3.1 Parties' Roles. Customer, as Controller, appoints Centercode, as a Processor, to Process the Personal Data on Customer's behalf. To the extent Customer is acting as Processor of the Personal Data, Customer appoints Centercode as Customer's sub-processor, which shall not change the obligations of either Customer or Centercode under this Addendum, as Centercode will remain a Processor with respect to Customer in such event and Customer will remain a Controller.

3.2 Purpose, Details, and Duration of Data Processing.

(a) Purpose of Processing. The purpose of the Processing of the Personal Data is the performance of the Services (including providing customer and technical support and as further instructed by Customer in connection with its use of the Services) and Customer hereby instructs Centercode to Process the Personal Data for the purposes set forth in the Agreement and this Addendum and/or as compelled by applicable law. Centercode shall Process the Personal Data only for the purposes set forth in the Agreement and this Addendum and only in accordance with the documented instructions of Customer, which may be specific instructions or instructions of a general nature as set out in this Addendum, the Agreement, or as otherwise notified by Customer (including by its Administrators) to Centercode from time to time, except where otherwise required by Applicable Data Protection Laws or as compelled by applicable law, court, or governmental order. Customer shall be responsible for ensuring that its instructions comply with Applicable Data Protection Laws.

(b) Details. The details of the Processing are set forth in Exhibit 1 (Details of Processing) to this Addendum. Except for limited Personal Data required for account creation, Customer, as Controller determines the categories of its data subjects and types of Personal Data it collects using the Services subject to the limitations in the Agreement. If Applicable Data Protection Laws and/or Customer's use of the Services requires modification to Exhibit 1 (Details of Processing), Customer will notify Centercode to request an amendment to Exhibit 1.

(c) Duration. Subject to the provisions of Section 4.5 (Data Deletion) to this Addendum or as otherwise agreed in writing by the parties, Centercode will Process the Personal Data for the duration of the Agreement.

3.3 Prohibition on Sale of Personal Data and CCPA Terms. Centercode will not "Sell" (as defined under Applicable US State Privacy Laws) or "Share" (as defined under the CCPA) the Personal Data. Centercode will not retain, use, or disclose the Personal Data for any purpose (including any "Commercial Purpose" as defined under the CCPA) except for the purpose described in this Addendum or as permitted under the CCPA. Centercode will not retain, use, or disclose the Personal Data outside the direct business relationship between Centercode and Customer, including by not combining any Personal Data with other personal data collected or received from another source, except as permitted by the CCPA. Centercode will enter into contractual agreements with its Sub-Processors that comply with the requirements under Applicable US State Privacy Laws relating to the sharing of Personal Data with third party contractors and sub-processors. Centercode will inform Customer if it determines that it can no longer meet its obligations under the CCPA or this Section 3.3 and will provide the same level of privacy protection as is required by the CCPA. If Centercode is engaged in unauthorized use of Personal Data, Customer may, upon reasonable notice to Centercode, take reasonable and appropriate steps to stop and remediate the unauthorized use of Personal Data. Centercode certifies that it understands the restrictions in the CCPA and this Section 3.3 and will comply with them.

3.4 Compliance with Laws. Each party warrants that it will comply with all requirements that apply to it under Applicable Data Protection Laws in connection with the Personal Data. If required to do so by a Supervisory Authority, each party may disclose the Addendum to such Supervisory Authority and such disclosure will not constitute a breach of confidence.

3.5 Controller Obligations. Customer shall be responsible for ensuring that, in connection with the Personal Data and its use of the Services, it has, and will continue to have, the right to transfer to Centercode, or provide Centercode access, to such Personal Data for Processing in accordance with the Agreement and this Addendum.

3.6 Customer Business Contact Data. Where Centercode Processes business contact details of Customer's employees, agents, and subcontractors for purposes of contract and customer relationship administration (the "**Customer Business Contact Data**"), it does so as a Controller and will do so strictly in accordance with Applicable Data Protection Laws. Customer shall be responsible for ensuring that it has, and will continue to have, the right to transfer to Centercode, or provide Centercode with access to, Customer Business Contact Data.

3.7 Data Transfer to Centercode and its Sub-Processors. Customer acknowledges and agrees that in performing the Services, Centercode receives Personal Data, which may include Personal Data that is subject to the protection of Applicable European Data Protection Laws, in the United States and in other jurisdictions in which it or its Sub-Processors have operations. Customer agrees that Centercode and its Sub-Processors may Process Personal Data in these jurisdictions in providing the Services to Customer under the Agreement. Centercode shall ensure its further onward transfers to its Sub-Processors are made in compliance with Applicable Data Protection Laws.

3.8 Compliance Reviews. Centercode shall reasonably cooperate with Customer to provide the information reasonably required by Customer for it to assess compliance with this Addendum to the extent required by Applicable Data Protection Laws. Customer shall pay its own costs of any such review or audit and any such review or audit shall take place in accordance with the following provisions:

(a) Any information provided by Centercode or its Sub-Processors is provided on a confidential basis.

(b) Audits and reviews under this Section 3.8 shall not take place more frequently than once per year with Customer combining and its requests with those of any Affiliates, unless otherwise required by Applicable Data Protection Laws.

(c) Centercode shall not be obligated to provide the information in a specific format, template, or portal, and Centercode shall not be obligated to enter into an agreement with any third party in connection with its compliance with this Section 3.8 and Centercode may comply with the request by providing its most recent independently validated security audits, including its SOC 2 report and penetration testing report summary to the extent those reports provide the information reasonably required by Applicable Data Protection Laws.

(d) Prior to any such review or audit, Customer and Centercode will discuss and agree in advance on the reasonable start date, scope, duration of, and security and additional confidentiality controls applicable to, the review or audit.

4. DATA PROTECTION

4.1 Security. Centercode shall implement and maintain appropriate technical and organizational measures designed to protect the Personal Data from a Security Incident, which at a minimum shall include standards no less stringent as those set forth in Exhibit 2.

4.2 Confidentiality. Centercode personnel (whether employee or contractor) authorized to Process the Personal Data and Centercode Sub-Processors shall be subject to a duty of confidentiality with respect to the Personal Data.

4.3 Training. Centercode personnel (whether employee or independent contractor) authorized to Process the Personal Data shall receive appropriate training regarding their responsibilities and obligations with respect to the Processing, protection, and confidentiality of the Personal Data.

4.4 Security Incidents. Upon becoming aware of a Security Incident, Centercode shall notify Customer without undue delay and pursuant to the terms of the Agreement, but within no more than forty-eight (48) hours and shall provide such timely information as Customer may reasonably request, including reasonable assistance to enable Customer to fulfill any data breach reporting obligations under Applicable Data Protection Laws, and to identify and remediate the cause of such Security Incident. Notification(s) of Security Incidents, if any, will be delivered as set forth in the Agreement or, if not provided in the Agreement, to one or more of Customer's Administrators by any means Centercode selects, including via email. Customer must ensure that Customer's Administrators maintain accurate contact information in Centercode's systems at all times.

4.5 Data Deletion. Upon termination or expiration of the Agreement, Centercode shall delete all Personal Data (including copies) in Centercode's possession in accordance with this Section 4.5, except to the extent that Centercode is required by applicable law to retain some or all of the Personal Data. Upon expiration or termination of Services, Centercode shall make the Personal Data available to Customer for retrieval for the period provided in the Agreement. No later than ninety (90) days after the expiration or termination of

Services, Centercode shall complete deletion of all the Personal Data on the Centercode Platform, with Personal Data in Centercode's backups deleted within thirty (30) days of deletion of that underlying data. Prior to that date, if Customer requires deletion, it must issue a written deletion request to Centercode, which serves to confirm that Customer is ready for Centercode to delete the Personal Data, in which case Centercode will delete Personal Data within seven (7) days of its receipt of such a written request, with Personal Data in backups deleted within thirty (30) days of deletion of the underlying data. In any period following expiration or termination of the Agreement during which Centercode is authorized to continue to Process the Personal Data under the Agreement or this Addendum, Centercode shall extend the protections of the Agreement and this Addendum to such Personal Data and limit any further Processing of such Personal Data to only those purposes that require the retention, for so long as Centercode maintains the Personal Data.

5. DATA SUBJECT OR SUPERVISORY AUTHORITY REQUESTS

5.1 Requests by Data Subjects or Supervisory Authorities Under Applicable Data Protection Laws. The Centercode Platform provides Customer with tools that may assist Customer in complying with its obligations under Applicable Data Protection Laws relating to responding to Data Subject Personal Data requests ("Data Subject Requests"). Customer is responsible for properly configuring the Services and using available controls in connection with the Services, including properly labeling data collection fields as Personal Data fields or not. To the extent that Customer is not reasonably able to respond to a Data Subject or Supervisory Authority request without assistance by Centercode, Centercode shall assist Customer as reasonably necessary to enable Customer to comply with Applicable Data Protection Laws. If Centercode must provide cooperation contemplated in this Section 5.1 that requires Centercode to take action that is outside of the scope of its ordinary Services and results in a material increase in the amount of time required by Centercode to perform the Services, Customer agrees to reimburse Centercode for commercially reasonable costs arising from this assistance. Any charge will be as agreed in writing between the parties.

5.2 Requests Made to Centercode. In the event a Data Subject or Supervisory Authority request or complaint is made directly to Centercode, Centercode shall promptly inform Customer, except to the extent prohibited by applicable law, by providing the full details of the request or complaint and Customer is responsible for responding to its Data Subjects, provided that Centercode may respond to a Data Subject request for data deletion that does not identify Customer with general instructions regarding the data deletion tools available within the Centercode Platform and to notify the Data Subject to contact the company operating the Centercode Platform implementation on which it has an account.

6. SUB-PROCESSING

6.1 Centercode's Sub-Processors. Customer expressly permits Centercode to engage Sub-Processors to Process the Personal Data on Centercode's behalf. Centercode's Sub-Processors are as identified in the Agreement and at https://www.centercode.com/legal/sub-processors from time to time. Centercode shall impose on such Sub-Processors written data protection terms that protect Personal Data to substantially the same standard provided for by this Addendum and shall remain liable for any acts or omissions of such Sub-Processors that cause Centercode to breach any of its obligations under the Addendum.

6.2 Changes to Sub-Processor List. In addition to Sub-Processor modifications authorized under the Agreement, Centercode may add or make changes to any approved Sub-Processor from time to time. Centercode shall provide Customer no less than thirty (30) days' notice of such changes (including by email to Customer's Administrators) provided that Customer subscribes to receive notifications of such updates at the https://centercode.com/legal/sub-processors. If Customer objects to the new or additional Sub-Processor on reasonable grounds relating to the protection of Personal Data, Customer may provide a written notice of objection to the appointment within fourteen (14) calendar days of such notice, in which case Centercode shall have the right to cure the objection through one of the following options (to be selected at Centercode's sole discretion):

(a) Centercode will cancel its plans to use the Sub-Processor to Process Customer's Personal Data or will offer an alternative to provide its Services without such Sub-Processor;

(b) Centercode will take the corrective steps reasonably requested by Customer in its objection (which remove Customer's objection) and proceed to use the Sub-Processor to Process Customer's Personal Data; or

(c) Centercode may cease to provide, or Customer may agree not to use, the aspect of the Services (temporarily or permanently) that would involve the use of such Sub-Processor to Process Customer's Personal Data.

If none of the above options is reasonably available and the objection has not been solved to the mutual satisfaction of the parties within thirty (30) days after Centercode's receipt of Customer's objection, either party may terminate the Agreement and Customer will be entitled to a pro-rata refund for any prepaid fees for the Service relating to the time period after the effective date of termination.

6.3 Emergency Sub-Processor Replacement. Centercode may replace a Sub-Processor if the reason for the change is beyond Centercode's reasonable control. In such an instance, Centercode shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-Processor as provided in Section 6.2.

7. PROVISIONS APPLICABLE TO PERSONAL DATA OF EUROPEAN RESIDENTS.

7.1 Applicability of Section 7. The additional terms and conditions in this Section 7 apply only with respect to European Personal Data.

7.2 Customer Instructions. Centercode will comply with the requirements in the Applicable European Data Protection Laws to notify Customer without delay if, in its opinion a documented instruction for the Processing of Personal Data given by Customer infringes Applicable European Data Protection Laws.

7.3 Cooperation. Taking into account the nature of Processing and the information available to Centercode, Centercode shall assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR and/or these obligations as may be contained in other Applicable European Data Protection Laws, to the extent Customer is unable to comply without such assistance, including providing Customer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under Applicable Data Protection Laws. Customer is responsible for determining the applicability of a data protection impact assessment and/or prior consultation with data protection authorities. If Centercode must provide cooperation contemplated in this Section 7.3 that requires Centercode to take action that is outside of the scope of its ordinary Services and results in a material increase in the amount of time required by Centercode to perform the Services, Customer agrees to reimburse Centercode for commercially reasonable costs arising from this assistance. Any charge will be as agreed in writing between the parties.

7.4 Transfers of European Personal Data. To the extent Centercode Processes Personal Data from Data Subjects who are subject to the protections of the Applicable European Data Protection Laws, Centercode shall not transfer the Personal Data of a Data Subject who is subject to the protections of the Applicable European

Data Protection Laws to any country or recipient not recognized as providing an adequate level of protection for Personal Data (as defined under the Applicable European Data Protection Laws) without ensuring that the transfer complies with the Applicable European Data Protection Laws. The parties agree to Process European Personal Data in compliance with the following:

(a) EEA Transfers. In relation to European Personal Data that is subject to the GDPR: (i) Customer is the "data exporter" and Centercode is the "data importer"; (ii) the Module Two terms apply to the extent the Customer is a Controller of European Personal Data and Module Three terms apply to the extent the Customer is a Processor of European Personal Data; (iii) the optional docking clause in Clause 7 does not apply; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with Section 6 of the Addendum; (v) the optional language in Clause 11 is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be the Republic of Ireland (without reference to conflicts of law principle); (vii) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in Exhibits 1 and 2 to this Addendum; and (viii) Standard Contractual Clauses shall supersede conflicting terms in the Agreement and this Addendum if and to the extent a Data Subject asserts rights as a third-party beneficiary regarding the Processing of his or her Personal Data. The parties agree that except as otherwise required by Applicable Data Protection Laws: (i) the audits described in Clauses 8.9 and 13 of the Standard Contractual Clauses shall be carried out in accordance with the specifications in Section 3.8 (Compliance Reviews) of the Addendum; and (ii) the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Centercode to Customer only upon Customer's request and that Clause 8.5 of the Standard Contractual Clauses will be satisfied by the return and/or deletion of data exporter's data in accordance with Section 4.5 (Data Deletion) of the Addendum.

(b) UK Transfers. In relation to European Personal Data that is subject to the UK GDPR: the Standard Contractual Clauses will apply as provided in Section 7.4(a) with the following modifications: (i) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK SCC Addendum, which will be incorporated into and form a part of the Standard Contractual Clauses; (ii) Tables 1, 2, and 3 of the UK SCC Addendum will be deemed completed with the information set out in Exhibits 1 and 2 to this Addendum; and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK SCC Addendum will be resolved in accordance with Section 10 and Section 11 of the UK SCC Addendum.

(c) Swiss Transfers. In relation to European Personal Data that is subject to the Swiss FDPA, the Standard Contractual Clauses will apply as provided in Section 7.4(a) with the following modifications: (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FDPA; (ii) references to "EU," "Union," and "Member State Law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "Swiss Federal Data Protection and Information Commissioner" and the "competent courts of Switzerland."

(d) Alternate Transfer Mechanism. Notwithstanding the foregoing, Centercode may terminate the Standard Contractual Clauses upon written notice to Customer if it offers an alternative transfer mechanism for transfers of European Personal Data to Centercode, Inc. that provides an equivalent level of protection and complies with Applicable European Data Protection Laws for the transfer of Personal Data outside of the EEA, the UK, or Switzerland (as the case may be).

8. AMENDMENTS

8.1 Amendment to this Addendum. Except as provided in the last sentence of this Section 8.1, this Addendum may only be amended by written agreement of the parties. If Centercode reasonably determines that modifications to this Addendum are required based on Applicable Data Protection Laws, Centercode may amend this Addendum as reasonably necessary to comply with Applicable Data Protection Laws by providing Customer with written notice of the amendment, and the amendment shall become effective and binding immediately upon notice to Customer.

9. MISCELLANEOUS

9.1 Customer agrees that it enters into this Addendum on behalf of itself and, to the extent required by Applicable Data Protection Laws, any of its Affiliates that is a Controller of the Personal Data and that is permitted to use the Services. Each such Affiliate agrees to be bound by the terms and conditions in this Addendum and the Agreement. Customer represents and warrants that it is authorized to enter into the Addendum on behalf of itself and, where applicable, all such Affiliates. Except to the extent prohibited by Applicable Data Protection Laws, only the entity that signs this Addendum as "Customer" shall have the right to exercise any rights or pursue any remedy under this Addendum.

9.2 Except as amended by this Addendum, the Agreement will remain in full force and effect. If any provision of this Addendum is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision shall be construed, as nearly as possible, to reflect the intentions of the invalid or unenforceable provision, with all other provisions remaining in full force and effect.

9.3 If there is a conflict between the Agreement and this Addendum, where the Addendum is applicable, the terms of this Addendum will control, provided however, that the Addendum and the Standard Contractual Clauses do not replace any additional rights related to Processing of Customer Data set forth in the Agreement.

9.4 Any claims brought under this Addendum, including the Standard Contractual Clauses, shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations, set forth in the Agreement.

9.5 Except in relation to a Data Subject's rights under the Standard Contractual Clauses regarding the Processing of his or her Personal Data or as may be required by Applicable European Data Protection Laws, the Agreement and this Addendum apply only between the parties hereto and do not confer any rights to any third-party Data Subjects.

9.6 Except in relation to the Standard Contractual Clauses to the extent required by Applicable European Data Protection Laws, this Addendum and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the law that governs the Agreement.

Exhibit 1 to Data Processing Addendum
Details of Processing

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as "Customer" in the parties' agreement to which the Standard Contractual Clauses are attached or incorporated by reference (the "Agreement") on behalf of itself and its affiliates that are permitted to use data importer's services (the "Services") pursuant to the Agreement.

Address: The Customer's address, as set out in the parties' Agreement and/or as set out in the Customer's account or billing details provided to data importer, or where Customer has executed this Addendum, as set forth in the execution page to this Addendum.

Contact person's name, position and contact details: The Customer's contact details, as set out in the parties' Agreement and/or as set out in the Customer's account or billing details provided to data importer, or where Customer has executed this Addendum, as set forth in the execution page to this Addendum.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with data exporter's use of the data importer's Services.

Role (controller/processor): Controller

Data importer(s):

Name: Centercode, Inc.

Address: 23422 Mill Creek Drive, Suite 105, Laguna Hills, CA 92653

Contact person's name, position and contact details: Luke Freiler, President, CEO, and Data Protection Officer, Centercode, Inc., 23422 Mill Creek Drive, Suite 105, Laguna Hills, CA 92653

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with data exporter's use of the data importer's Services.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Data exporter may submit Personal Data in the course of using the Services as determined and controlled by the data exporter in its sole discretion subject to prohibitions contained in the Agreement, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

customers and customer prospects of the data exporter; employees and contractors of the data exporter; participants or prospective participants in product and service tests (e.g., Beta and Delta tests) performed by or on behalf of data exporter, and other end-users

Categories of personal data transferred:

Data exporter may submit Personal Data in the course of using the Services as determined and controlled by the data exporter in its sole discretion subject to prohibitions contained in the Agreement, and which may include but is not limited to the following categories of Personal Data:

full name, user identification, title, position, employer, email, phone number, address, gender, age, date of birth, professional life data, personal life data, connection data, location data, preferences, opinions, device or service ownership, possession and/or usage data, experiential data, photographs, audio, video, and any other personal data submitted by data exporter or its end users using the Services

Sensitive data transferred and applied restrictions or safeguards:

None. Data exporter is not permitted to collect "sensitive data" pursuant to the terms of the parties' Agreement.

The frequency of the transfer:

Continuous

Nature of the processing:

Processing activities in the performance of the Services (including providing customer and technical support and as further instructed by data exporter in connection with its use of the Services) as set forth in the Agreement and/or as compelled by applicable law. Data exporter instructs data importer to Process Personal Data for these purposes in the countries in which data importer or its Sub-Processors maintain facilities as necessary for the provision of the Services as identified in the Data Processing Addendum.

Purpose of the data transfer and further processing:

Data importer will process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the parties' order form and as further instructed by data exporter in its use of the Services.

The period for which the personal data will be retained:

Data importer will process the Personal Data for the duration of the Agreement, including any period following the end of the Agreement designated for transition of Services and data as specified in the Agreement, unless otherwise agreed in writing.

Sub-Processors:

Centercode's Sub-Processors, including contact information and a description of the processing, are as identified in the Agreement and at https://www.centercode.com/legal/sub-processors.

For transfers to (sub-) processors, the subject matter, nature and duration of the processing:

The subject matter, nature, and duration of the processing are described in the parties' Data Processing Addendum.

C. COMPETENT SUPERVISORY AUTHORITY

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority shall be as determined in accordance with the GDPR.

Exhibit 2 to Data Processing Addendum

Centercode Security Standards

Customer is responsible for reviewing the information made available by Centercode relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and contractors follow appropriate guidelines regarding data security.

I. Centercode Platform Security

A. Data Storage, Security and Availability

1. Secure Storage

Centercode stores all Personal Data on cloud servers that are in a physically secure data center in the United States (unless a different location is expressly identified in the Agreement), as identified in the Agreement. Centercode shall ensure that any such data center is covered by a third-party security audit, such as ISO/IEC 27001, or SOC 2, Type 2 and shall provide Customer evidence of such audit upon request after execution by Customer of the data center's standard non-disclosure agreement.

Each data center holding the Personal Data maintains physical security features including the following:

- On-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week
- Monitoring of Video/Closed Circuit TV cameras and all alarm systems
- Regular internal and external security personnel monitoring of the data center
- Formal access procedures for allowing physical access to the data center, including:
    - An access control system using keycard/badge devices and biometric authentication, with two-factor authentication to gain access
    - Self-locking and alarmed facility entrances/exits
    - Logging of facility entrances/exits

2. Availability

Appropriate measures are taken against accidental destruction or loss of Personal Data, including backup of all Personal Data on a regular basis. Centercode's Service Level Agreement (available at https://www.centercode.com/sla) contains response and resolution commitments to Centercode Platform customers with annual or greater Service terms. In addition, the data center environment is designed with features for minimizing the impact of external environmental risks, including:

- Uninterruptible power supply (UPS) systems
- Diesel generators for backup power
- Fire detection and prevention systems
- 24x7 network operations center monitoring
- Redundant HVAC equipment

Centercode maintains a business continuity/disaster recovery plan that identifies and addresses risk factors associated with the Services.

3. Third-Party Network Penetration Test

Centercode shall have a third-party network penetration test performed annually. All critical vulnerabilities shall be remediated within thirty (30) days of identification to the extent reasonably possible. Centercode shall provide Customer an executive summary of such test upon request.

4. Vulnerability Scans

Centercode (either directly or through third parties) shall scan all internet-accessible sites related to Customer's Services at least annually and at any time a major change is made to a hosted site that could introduce vulnerabilities using industry standard scanning tools such as Nessus.

5. Access Controls

Additional measures are taken to protect against unauthorized access to the IT systems holding the Personal Data and to the Personal Data including:

- Production systems behind stateful inspection firewall
- Intrusion detection systems
- Access rights assigned based on job role with management approval of new/modified access
- Terminated personnel access disabled within 24 hours
- Regular access review for personnel with access to production systems or Personal Data
- Password requirements and procedures for Centercode personnel
- No access for guest users or anonymous accounts
- Access to IT systems at data center restricted to appropriate individuals

6. Database and Disclosure Controls

Measures are taken to protect against unauthorized access, alteration, and removal of Personal Data during transport and otherwise, including:

- Customer Data on production systems is logically segregated into a separate database
- Data encryption in transit using the most current version of HTTPS/TLS
- Encryption of backups using AES-256
- Encryption at rest of Customer Data on the Centercode Platform using AES-256
- Dedicated cloud-based servers are available to customers with select Editions and with annual or greater subscription terms where expressly purchased by the Customer, as specified in Customer's Agreement

B. Centercode Personnel

Measures are taken to ensure the reliability of any Centercode personnel engaged in the Processing of the Personal Data, including:

- Appropriate background checks to the extent legally permissible in accordance with local labor law and statutory regulations
- Execution of confidentiality agreements
- Regular personnel training appropriate to role and access, including security and data privacy training

C. Change Management and Maintenance

Measures are taken to log, test, and approve material changes to production systems, including:

- Testing and approval of critical/material application changes prior to implementation into production
- Restriction of access for migrating changes into production environments to appropriate individuals
- Regular review of critical changes to confirm appropriateness and authorization
- Local deployment of scheduled maintenance, patches, and material application changes in test environment prior to being introduced to production environment
- Customer notification prior to scheduled maintenance
- Backup of all data on servers hosting production systems prior to major updates

D. Customer Access Control and Privilege Management

Customer is responsible for ensuring the security of access by its end users to the Services. The Services include features that enhance Customer's ability to self-manage access controls and privileges, including:

- Customer's administrators and end-users must authenticate themselves in order to use the Service
- Prior to display of data to an authorized end-user or administrator, login and password credentials are validated
- Password complexity standards default to an eight-character minimum with alpha and numeric requirements and prohibitions on using other identity fields (username, first and last name, or email) within the password, but these settings can be easily modified by the platform administrators to add additional characters and complexity requirements
- Passwords are stored in encrypted form (AES/128 bit)
- Passwords cannot be retrieved or viewed by anyone, including Centercode
- Where SSO integration is purchased or included in the edition Customer has ordered, Customer can optionally integrate its own single sign-on system (such as SAML) with its Centercode Platform implementation, and where the single sign-on system supports 2-factor authentication, Customer can extend this feature to its access to the Services
- By default, Customer's users on its Centercode Platform implementation may attempt three invalid password attempts before account is locked for a period of time
- Any modifications to Customer user's personal account on its Centercode Platform implementation will email the user to inform the user of the change
- Role-based access, allowing Customer administrators on Customer's Centercode Platform implementation to define access for Customer's users
- Logical isolation of data on a per-user basis, with user security access checked prior to loading every individual page
- HTTPS encryption (also referred to as TLS connection) is required to use the Services (non-secure links are redirected to HTTPS equivalents)

E. Request and Incident Tracking, Monitoring and Logging

When a request is made to Centercode Support from a customer, a ticket is created in Centercode's internal request tracking system and progress is tracked until final resolution. A similar system will be used to track any Security Incidents. Centercode monitors and logs access to the production systems and logs are maintained for at least ninety days.

F. Centercode Sub-Processors

Prior to onboarding of any Sub-Processor and on an annual basis, Centercode conducts a review of the security and practices of the Sub-Processor to ensure an appropriate level of security. The Sub-Processor is required to enter into appropriate written security, confidentiality, and privacy contract terms with Centercode consistent with the requirements of Applicable Data Protection Laws.

Some editions and/or purchased feature sets of the Centercode Platform offer the ability for Customer to integrate it with, and share data with, other systems ("**Centercode Platform Integrations**"). With Centercode Platform Integrations, Customer can automatically exchange Centercode Platform data to and from Customer's and third parties' systems, platforms, and applications (in Customer's discretion) without the need for manual duplication of data.

If Customer enables and uses Centercode Platform implementations to move Personal Data from the Centercode Platform to the systems, platforms, or applications of third parties, Customer (and not Centercode) is sharing this Personal Data with these third parties. **Customer understands and agrees that these third parties are Customer's Processors and not Centercode's Sub-Processors** even if Centercode, at Customer's request, assists Customer in integrating a third-party system, platform, or application. Customer is the party responsible for ensuring that it has appropriate terms in place with each of these Sub-Processors that are compliant with Applicable Data Protection Laws.

Professional Services Exhibit to Data Processing Addendum

If and where the Services involve the performance by Centercode of Professional Services (as specified in a mutually executed Order Form), Centercode and Customer understand and agree that the standards and commitments set forth in the Data Processing Addendum and its exhibits are modified as provided in this Professional Services Exhibit.

1. Additional Security Provisions and Sub-Processors for Professional Services

To perform Professional Services for Customer, in some circumstances Centercode needs to remove Personal Data from the Centercode Platform production systems to other Centercode systems (or the systems of Centercode's Sub-Processors) in order to perform the Services or at the request of Customer. In this event, Centercode will remove the Personal Data only to the extent necessary to perform the services or respond to Customer's request and will abide by internal policies governing the handling of Personal Data removed from the production systems. These policies are designed to ensure that the Personal Data is only accessible by Centercode employees, contractors, and Sub-Processors as necessary to perform the Professional Services. When the Personal Data is removed from the production systems, Centercode maintains a record of the location(s) of the Personal Data. Please review Centercode's Sub-Processors at https://www.centercode.com/legal/sub-processors to better understand the additional Sub-Processors for Professional Services customers.

2. Supplemental Data Protection Terms for Certain Professional Services – Data Sharing Arrangement

For the avoidance of doubt, this Section 2 only applies where Customer is acting as a Controller of Betabound Personal Data shared by Centercode with Customer as described in Section 3.1 of the Data Processing Addendum.

Where Centercode discloses Betabound Personal Data to Customer in connection with Professional Services (as opposed to the Participant sharing its own Personal Data with the Customer directly), it agrees to Process the Betabound Personal Data in accordance with the terms of the Agreement and this Section 2.

2.1 In connection with Services involving Data Subjects from Centercode's Betabound community of test participants, where Centercode (in its capacity as a Controller) transfers to Customer or provides Customer with access to Betabound Personal Data for Customer to Process, it does so for the purpose(s) specified in Appendix 1 to this Professional Services Exhibit (the "Purpose") and Customer shall not use the Betabound Personal Data except for the Purpose.

2.2 Each party shall comply with Applicable Data Protection Laws in carrying out their obligations with respect to the Betabound Personal Data, including those under this Professional Services Exhibit. Customer will not: (a) "Sell" (as defined under Applicable US State Privacy Laws) or "Share" (as defined under the Applicable US State Privacy Laws) the Betabound Personal Data; (b) retain, use, or disclose the Betabound Personal Data for any purpose (including any "Commercial Purpose" as defined under the CCPA) except for the Purpose; (c) retain, use, or disclose the Betabound Personal Data outside the direct business relationship between Centercode and Customer, including by not combining any Betabound Personal Data with other personal data collected or received from another source, except as permitted by Applicable US State Privacy Laws.

2.3 Customer will provide the same level of privacy protection as is required by Applicable Data Privacy Laws. If Customer is engaged in unauthorized use of Betabound Personal Data, Centercode may, upon reasonable notice to Customer, take reasonable and appropriate steps to stop and remediate the unauthorized use of Betabound Personal Data. Customer certifies that it understands the restrictions in the CCPA and will comply with them.

2.4 Customer will, upon Centercode's request, assist Centercode in its response to a consumer's request to exercise a right it has under Applicable Data Protection Laws with respect to the Betabound Personal Data. Customer will allow Centercode to take reasonable and appropriate steps to ensure Customer uses and protects the Betabound Personal Data in a manner consistent with Centercode's obligations under Applicable Data Protection Laws.

2.5 If Customer is no longer able to Process the Betabound Personal Data in a manner that is consistent with Applicable Data Protection Laws and this Professional Services Exhibit, it shall immediately inform Centercode and advise Centercode of any steps it proposes to take to remediate any such inconsistency. If requested by Centercode, Customer shall immediately suspend any inconsistent Processing.

2.6 Centercode will not transfer any Betabound Personal Data to Customer except as specifically contemplated by the terms of the Agreement, this Professional Services Exhibit, and Applicable Data Protection Laws.

2.7 If required to do so by a Supervisory Authority, Customer acknowledges and agrees that Centercode may disclose the Data Processing Addendum, including this Professional Services Exhibit, to such Supervisory Authority and that such disclosure will not constitute a breach of confidence.

2.8 As a minimum, each party's privacy policy shall comply with Applicable Data Protection Laws and each party shall ensure where acting in its capacity as a Controller, that it brings its privacy policy (and any amendments) to the attention of Data Subjects.

2.9 Customer may only transfer the Betabound Personal Data from a country within the EEA, the UK, or Switzerland to a non-Adequate Country or Sector if Customer has provided appropriate safeguards by entering into Standard Contractual Clauses, or by relying on Binding Corporate Rules applicable to Customer and, at Centercode's request, Customer will provide a copy of the transfer mechanism it relies on.

2.10 Notwithstanding termination of the Agreement for any reason, Customer shall continue to protect the Betabound Personal Data it received prior to termination to the standard required by this Professional Services Exhibit, including as required under Applicable Data Protection Laws on an ongoing basis. If Customer is unable to do so, it must immediately inform Centercode and at Centercode's request either delete or return all such Betabound Personal Data in its possession or control. This provision shall survive termination of the Agreement, the Data Processing Addendum, and this Professional Services Exhibit.

2.11 Each party shall be responsible for responding to any request, correspondence, inquiry, or complaint made directly to it regarding its Processing of the Betabound Personal Data but shall inform the other (to the extent the other may be implicated in the request) of the request and how it intends to respond, unless prohibited from doing so by Applicable Data Protection Laws.

2.12 Each party shall implement appropriate technical and organizational measures in accordance with Appliable Data Protection Laws, including Article 32 of the GDPR, to ensure the security of the Betabound Personal Data and protect it against any unauthorized and unlawful Processing, and against a Security Incident.

2.13 If Customer discovers or is notified of any Security Incident relating to the Betabound Personal Data, it shall notify Centercode without undue delay and in any event within forty-eight (48) hours and keep Centercode updated regarding the investigations into the Security Incident and the remedial actions it is taking, unless prohibited from doing so by applicable law. Notification(s) of Security Incidents, if any, will be delivered as agreed in the Agreement or, if not provided in the Agreement to security@centercode.com.

2.14 Customer shall not retain or Process the Betabound Personal Data for longer than is necessary to carry out the Purpose.

2.15 Customer shall ensure that subcontractors it appoints to Process the Betabound Personal Data provide at least the same level of protection for the Betabound Personal Data and the rights of Data Subjects as Customer is obligated to provide under this Professional Services Exhibit and Applicable Data Protection Laws. Each such subcontractor must be subject to a written agreement that is compliant with Applicable Data Protection Laws and that imposes obligations at least as restrictive as those imposed on Customer under this Professional Services Exhibit. Customer will remain fully responsible and liable to Centercode for the performance of those obligations by each subcontractor. Customer shall further ensure that any such subcontractor only Processes the Betabound Personal Data in accordance with Customer's instructions and those instructions are consistent with the Purpose.

2.16 Customer shall ensure the reliability of any person that it authorizes to Process the Betabound Personal Data (including its employees and contractors) and that each such person is subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty). Customer shall not permit any person to Process the Betabound Personal Data who is not under such a duty of confidentiality. Customer shall ensure that all such authorized persons Process the Betabound Personal Data only as permitted by this Professional Services Exhibit and Applicable Data Protection Laws.

APPENDIX 1 TO PROFESSIONAL SERVICES EXHIBIT

DATA SHARING

This Appendix 1 to the Professional Services Exhibit forms part of the Data Processing Addendum where the Professional Services Exhibit is applicable and describes the Processing that Customer will perform as a Controller.

Purpose

The Purpose of the transfer of Betabound Personal Data to Customer is to enable Customer to use the Betabound Personal Data in connection with Customer's internal use of Services deliverables (test results and feedback) relating to its product and service testing (e.g., Beta and Delta testing).

Personal Data

Customer is Processing the following categories of Betabound Personal Data in connection with the Purpose:

Data Subjects:

Members of Centercode's community of prospective test participants commonly known as its "Betabound Community"

Categories of Personal Data:

Includes full name, user identification, title, position, employer, email, phone number, address, gender, age, date of birth, professional life data, personal life data, connection data, location data, preferences, opinions, device or service ownership, possession and/or usage data, experiential data, photographs, audio, and video

Centercode is not transferring to Customer any Betabound Personal Data that is Sensitive Personal Data

Processing operations

Processing activities are those that occur in the use by Customer of the Services and Service deliverables related to Customer's product and service testing (e.g., Beta and Delta testing). The transfer of Betabound Personal Data may occur from time to time or continuously during the Services term.