DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**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 contracts.

CENTERCODE, INC., a California corporation **By:**  _____ **Name: Luke Freiler** **Title: Chief Executive Officer** **Signature Effective Date: May 25, 2018** **Address:** **23332 Mill Creek Drive, Suite 260** **Laguna Hills, CA 92653** **Attn: CEO**	**CUSTOMER NAME:** _____ (full legal entity name) **By (Sign Here):** _____ **Printed Name:** _____ **Title:** _____ **Date:** _____ **Customer Address:** _____ _____ _____ **Attention:** _____

This Addendum includes the Data Processing Terms and the attached Annex 1 (Centercode Security Standards), Annex 2 (Standard Contractual Clauses), and Annex 3 (Supplemental Data Protection Terms - Data Sharing Arrangement), and supplements and amends Customer's agreement(s) (the "**Agreement**") with Centercode for the provision of Services (as defined below) by Centercode in relation to EU Personal Data (as defined below) and, to the extent applicable, Betabound EU Data. This Addendum will be effective as of the day that Centercode receives a complete and executed Addendum from Customer in accordance with the following instructions, or if later, the date of the parties' Agreement (the "**Addendum Effective Date**").

INSTRUCTIONS

This Addendum (including the Standard Contractual Clauses, defined below) has been pre-signed on behalf of Centercode. To enter into this Addendum, Customer must:

(1) complete the table above by signing and providing the customer full legal entity name, address, and signatory information;

(2) sign and provide the signatory information in the three locations required on the Standard Contractual Clauses (Annex 2 to this Addendum), completing Appendix 1 to Annex 2 as applicable;

(3) complete Appendix 1 to Annex 3 as applicable; and

(4) submit the complete and signed Addendum to Centercode via email to gdpr@centercode.com.

This Addendum will be effective only if it is executed and submitted to Centercode in accordance with these instructions and all items in the table above are completed accurately and in full. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void.

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.

"Betabound EU Data" means Personal Data, the Processing of which is subject to the Data Protection Legislation, of members of Centercode's Betabound Community of test participants that is Controlled by Centercode and is received by Customer or its Affiliates from Centercode in connection with the Services, and for which Customer or its Affiliates is deemed to be a Data Controller.

"**Customer**" means the non-Centercode party to both the Agreement and this Addendum that has access to the Services.

"**Customer Data**" means the data that Customer submits or provides to Centercode in the course of using the Services, or collects directly from users through its use of the Services (in either case, not including Customer Business Contact Data (defined below)).

"**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Processing**", and "**Supervisory Authority**" shall be interpreted in accordance with the Data Protection Legislation;

"**Data Protection Legislation**" means the GDPR and all other applicable laws relating to processing of Personal Data and privacy that may exist in the EEA, the UK or Switzerland and any legislation and/or regulation made pursuant to the GDPR, or which amends, replaces, re-enacts or consolidates the GDPR;

"**EEA**" means the European Economic Area, which for the purposes of this Addendum, includes the United Kingdom;

"**EU Personal Data**" means any Customer Data that constitutes Personal Data, the Processing of which is subject to Data Protection Legislation, that is Controlled by Customer and its Affiliates and their respective customers or other users (where applicable), which Centercode Processes in the course of providing the Services under the Agreement, wherever the Processing takes place.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

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

"**Standard Contractual Clauses**" means Annex 2 attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, including any applicable national implementations thereof.

2. APPLICABILITY OF THIS ADDENDUM

2.1 Applicability. This Addendum shall apply only to the extent Customer is established within the EEA or Switzerland and/or to the extent Centercode Processes EU Personal Data of Data Subjects located in the EEA or Switzerland on behalf of Customer or a Customer Affiliate in connection with the Services.

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 Data Controller, appoints and instructs Centercode, as a Data Processor, to Process the EU Personal Data on Customer's behalf. To the extent Customer acts as a Data Processor of the EU Personal Data, Customer appoints Centercode as Customer's sub-processor, which shall not change the obligations of either Customer or Centercode under this GDPR Addendum, as Centercode will remain a Data Processor with respect to Customer in such event. Where Customer Processes Betabound EU Data it receives or has access to in connection with the Services and is deemed to be a Data Controller to that data, it agrees to Process such data in accordance with the terms set out in Annex 3 (Supplemental Data Protection Terms - Data Sharing Arrangement).

3.2 Instructions for and Purposes of Data Processing. The purpose of the Processing of the EU Personal Data is the performance of the Services and Customer hereby instructs Centercode to Process the EU Personal Data for the purposes set forth in the Agreement and this Addendum. Centercode shall Process the EU 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 to Centercode from time to time), except where otherwise required by applicable law. Centercode will comply with the requirements in the GDPR to notify Customer immediately if, in its opinion, an instruction for the Processing of EU Personal Data given by Customer infringes applicable Data Protection Legislation.

3.3 Compliance with Laws. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this Addendum, including all applicable statutory requirements relating to data protection.

3.4 Data Controller Obligations. Customer, as Data Controller, shall be responsible for ensuring that, in connection with EU 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 the EU Personal Data for Processing in accordance with the terms of the Agreement and this Addendum. If required to do so by a Supervisory Authority, Customer may disclose the Data Processing Addendum to such Supervisory Authority and such disclosure will not constitute a breach of confidence.

3.5 Customer Business Contact Data. Where Centercode Processes business contact details of Customer's employees, agents, and subcontractors (the "**Customer Business Contact Data**") as Data Controller for

purposes of contract and customer relationship administration, it will do so strictly in accordance with the Data Protection Legislation and 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.

4. DATA PROTECTION

4.1 Security. Centercode shall implement and maintain appropriate technical and organizational measures designed to protect the EU Personal Data from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the EU Personal Data (each, a "**Security Incident**"), which at a minimum shall include the standards set forth in Annex 1.

4.2 Training. Centercode shall ensure that its relevant employees, agents, and contractors receive appropriate training regarding their responsibilities and obligations with respect to the Processing, protection, and confidentiality of EU Personal Data.

4.3 Confidentiality. Centercode shall ensure that any person that it authorizes to Process the EU Personal Data (including employees, agents, and subcontractors) shall be subject to a duty of confidentiality (whether contractual or statutory).

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 require to enable Customer to fulfill any data breach reporting obligations under the Data Protection Legislation. Centercode will take steps to immediately 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 or make available to Customer for retrieval all EU Personal Data (including copies) in Centercode's possession, except to the extent that Centercode is required by applicable law to retain some or all of the EU Personal Data. Following expiration or termination of Services, Centercode shall make the EU Personal Data available to Customer for retrieval for the period provided in the Agreement. Ninety (90) days after the expiration or termination of Services, Centercode shall complete deletion of all the EU Personal 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 EU Personal Data, in which case Centercode will delete EU Personal Data within seven (7) days of its receipt of such a written request. EU Personal Data in backups will be 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 EU Personal Data under the Agreement or this Addendum, Centercode shall extend the protections of the Agreement and this Addendum to such EU Personal Data and limit any further Processing of such EU Personal Data to only those purposes that require the retention, for so long as Centercode maintains the EU Personal Data. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Centercode to Customer only upon Customer's request and that Clause 12(1) of the Standard Contractual Clauses will be satisfied by the return and/or deletion of data exporter's data in accordance with this Section 4.5, except to the extent otherwise required by applicable law. In the case of Services involving a Common Implementation (as defined in Annex 1) or Managed Customer Validation Services (as defined in Annex 1), the obligations in this Section 4.5 are modified as described in Annex 1, Section II(B) (Managed Customer Validation Services and Common Implementation Customers; Data Deletion).

5. SUB-PROCESSING

5.1 Centercode's Sub-Processors. Customer agrees that Centercode may engage third-party sub-processors (collectively, "**Sub-processors**") to Process the EU Personal Data on Centercode's behalf. The Sub-processors currently authorized to be engaged by Centercode and authorized by Customer are listed in Annex 1 and Customer hereby consents to Centercode's use of such Sub-processors. Centercode shall impose on such Sub-processors data protection terms that protect the EU Personal Data to the same standard provided for by this Addendum and shall remain liable for any breach of the Addendum caused by a Sub-processor.

5.2 Changes to Sub-processor List. Centercode may, by giving no less than thirty (30) days' written notice to Customer, add or make changes to the Sub-processors referenced in Annex 1. Without prejudice to any termination rights Customer has under the Agreement, Customer may provide a written notice of objection to the appointment of an additional or substitute Sub-processor on reasonable grounds relating to the protection of EU Personal Data 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-contractor with regard to Customer's EU 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 with regard to Customer's EU Personal Data; or

(c) Centercode may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-processor with regard to its EU Personal Data, subject to a mutual agreement of the parties to adjust the fees for the Services considering the reduced scope of the Services.

If none of the above options are 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 prepaid fees for Services not performed as of the date of termination.

5.3 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 5.2.

6. CENTERCODE COOPERATION

6.1 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, including as follows:

(a) Data Subjects' Rights. Centercode shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under the Data Protection Legislation, including rights of access, correction, restriction, objection, erasure, or data portability, as applicable. Customer is responsible for properly configuring the Services and using available controls in connection with the Services described at https://centercode.com/gdpr. In the event a Data Subject inquiry, communication, or request is made directly to Centercode, Centercode shall promptly inform Customer by providing the full details of the request and Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure, or data portability of that Data Subject's EU Personal Data.

(b) Data Protection Impact Assessments and Prior Consultation. Centercode shall provide Customer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under the Data Protection Legislation. Customer is responsible for determining the applicability of a data protection impact assessment and/or prior consultation with data protection authorities.

6.2 Out of Scope Services. Customer accepts that if Centercode must provide cooperation contemplated in this Section 6 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, Centercode may wish to make a reasonable charge, in which case that charge will be as agreed in writing between the parties.

6.3 Security Audits. Except to the extent provided to the contrary in the Agreement, any security or compliance review or audit shall take place at Customer's cost and in accordance with the following provisions:

(a) Centercode shall reasonably cooperate with Customer in connection with any review or audit by Customer relating to matters under this Addendum to the extent required by the Data Protection Legislation.

(b) 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 confidentiality controls applicable to, such review or audit.

(c) The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the specifications in this Section 6.3 unless the Agreement or the requirements of applicable law provide otherwise.

7. STANDARD CONTRACTUAL CLAUSES

7.1 Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to EU Personal Data that is transferred outside the EEA or Switzerland, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for EU Personal Data. The Standard Contractual Clauses will not apply to EU Personal Data that is not transferred, either directly or via onward transfer, outside the EEA or Switzerland.

7.2 Conflicting Terms. The Standard Contractual Clauses in Annex 2 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.

7.3 Termination of Standard Contractual Clauses. Centercode may terminate the Standard Contractual Clauses if it offers alternative means to Customer that provide an equivalent level of protection and that comply with the Data Protection Legislation for the transfer of Personal Data outside of the EEA or Switzerland to any country not deemed by the European Commission as providing an adequate level of protection.

8. MISCELLANEOUS

8.1 Except as amended by this Addendum, the Agreement will remain in full force and effect.

8.2 If there is a conflict between the Agreement and this Addendum, 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.

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

8.4 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 the Data Protection Legislation, the Agreement and this Addendum apply only between the parties hereto and do not confer any rights to any third party Data Subjects.

8.5 Except in relation to the Standard Contractual Clauses to the extent required by the Data Protection Legislation and/or applicable 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.

Annex 1

Centercode Security Standards

Centercode and Customer understand and agree that the following security measures apply under the Data Processing Addendum to Customer's Services with respect to EU Personal Data. **Nothing herein is intended or shall be construed to limit Centercode's obligations to Customer as specified under the Agreement.**

If and where the Services include access by Customer to a shared (and not customer branded) database implementation of the Centercode Platform (a "**Common Implementation**") or the performance by Centercode of managed Alpha, Beta, or Field Test ("**Managed Customer Validation**") Services. Centercode and Customer understand and agree that the standards and commitments in the Data Processing Addendum and this Annex 1 are modified as set forth in Section II (Managed Customer Validation Services and Common Implementation Customers) of this Annex 1.

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 EU Personal Data on cloud servers that are located in a physically secure data center in the United States, as identified in Section I(F) (Centercode Platform Sub-processors) below. 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 EU 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 key-card/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 EU Personal Data, including backup of all EU Personal Data on a regular basis. Centercode's Service Level Agreement to Centercode Platform customers (available at https://www.centercode.com/sla) contains response and resolution commitments. 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 EU Personal Data and to the EU 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 EU 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 EU 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
- Where expressly included in Customer's Agreement governing such Services, encryption at rest of Customer Data using AES-256
- Dedicated cloud-based servers available where expressly included in Customer's Agreement governing such Services

B. Centercode Personnel

Measures are taken to ensure the reliability of any Centercode personnel engaged in the Processing of the EU 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 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
- 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 may attempt three invalid password attempts before their account is locked for a period of time
- Any modifications to Customer user's personal account will email the user to inform the user of the change
- Role-based access, allowing Customer administrators 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. This same 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 Platform Sub-processors

Prior to onboarding of any Sub-processor, 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 security, confidentiality, and privacy contract terms consistent with the requirements of the Data Protection Legislation. Customer approves the use by Centercode of the following Sub-processors:

- Data Center/Cloud Services - Amazon Web Services, Inc. (US-based locations, unless otherwise specified in the Agreement); and

- Any Sub-processor appointed pursuant to the Data Processing Addendum.

The Centercode Platform is designed to enable Customer to integrate it with, and share data with, other systems ("**Centercode Platform Integrations**"). If Customer enables and uses 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 the Data Protection Legislation.

II. Managed Customer Validation Services and Common Implementation Customers

Unless Customer's Agreement expressly states that Centercode will perform Managed Customer Validation Services on Customer's own branded and subscribed Centercode Platform implementation, Managed Customer Validation Services are performed on a Common Implementation (defined above). If and where the Services include a Common Implementation or involve the performance by Centercode of Managed Customer Validation Services, Centercode and Customer understand and agree that the standards and commitments set forth in the Data Processing Addendum and this Annex 1 are modified as follows:

A. Secure Storage of Data Removed from the Platform

In order to perform Managed Customer Validation Services for Customer, whether on a Common Implementation or Customer's own implementation of the Centercode Platform, in some circumstances Centercode needs to remove EU Personal Data from the 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 EU 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 EU Personal Data removed from the production systems. These policies are designed to ensure that the EU Personal Data is only accessible by Centercode employees, contractors,

and Sub-processors as necessary to perform the Managed Customer Validation Services. When EU Personal Data is removed from the production systems, Centercode maintains a record of the location(s) of the EU Personal Data. EU Personal Data removed from the production systems is located in the United States, where Centercode is located, and at the locations of its Sub-processors, identified below in Section II(E).

B. Data Deletion

For Managed Customer Validation Services performed on a Common Implementation, Centercode commits to deleting Customer's EU Personal Data at the end of Services. Because the Services end-date is often fluid, Centercode requires its Managed Customer Validation Services customers to provide a written request to begin the account deletion process. EU Personal Data deletion requests will be handled by deleting all of the users provided to Centercode by Customer (i.e. from the proprietary user lists supplied by Customer), which deletes the user identity and the data in fields identified as Personal Data fields, leaving the remaining data re-associated with an anonymized User Account containing no EU Personal Data.

In addition, Centercode's Managed Customer Validation Services team adopts best practices to ensure that EU Personal Data is only collected in fields marked as Personal Data fields. EU Personal Data will be deleted within 90 days of Customer's request for deletion. Optionally, Customer may request for its EU Personal Data be deleted sooner, in which case Centercode will expedite the deletion process to remove all EU Personal Data within 7 days of the request (with backups being purged within 30 days).

C. Services Access and Platform Administration

For Managed Customer Validation Services conducted by Centercode on a Common Implementation, Centercode is the platform Administrator. In this situation, Customer manages access to its Customer Data and to its Services by notifying Centercode about which individuals it wishes to assign to Customer's internal access "team." Password complexity standards are set to an eight-character minimum with alpha and numeric requirements, and access cannot be integrated with Customer's own single sign-on system.

D. Shared Database

The Common Implementation is a shared database with data programmatically isolated between Centercode customers. Dedicated cloud-based infrastructure is not available in this environment. Encryption at rest of data located on the Common Implementation infrastructure is available where the Customer's Agreement for the Common Implementation Services expressly provides for encryption of such data at rest.

E. Managed Services Sub-processors

In addition to the cloud-based hosting providers identified above in "Centercode Platform Sub-processors," Centercode uses G-Suite for general office services. Google LLC is therefore a Sub-processor for Centercode's Managed Customer Validation Services customers with data center locations set forth at https://www.google.com/about/datacenters/inside/locations/index.html. In addition, depending on the Managed Customer Validation Services ordered by Customer, Centercode may also use additional Sub-processors identified at https://centercode.com/gdpr under the section entitled "Managed Services Sub-Processors" (as may be updated by Centercode from time to time).

Centercode has appropriate and compliant data processing terms in place with all of its Sub-processors that process EU Personal Data. In addition, where Customer engages Centercode to perform shipping services on behalf of Customer, the contact information and shipping address of the recipient is provided to the shipping provider on behalf of Customer, as is always the case when shipping.

Where, as a part of the Managed Customer Validation Services (including services performed using the Common Implementation), Customer directs or approves the use of any Centercode Platform Integration, Personal Data may move from the Centercode Platform to the systems, applications, and/or platforms of these third parties. In this case, the third party receiving the data will be the Sub-processor of Centercode only where Centercode (as opposed to Customer) is the party with the account/contractual relationship with that third party relating to those services. Where Customer has the account/contractual relationship with that third party, however, Customer understands and agrees that these third parties are Customer's Processors and not Centercode's Sub-processors.

Annex 2

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

the entity identified as the "**Customer**," in the Data Processing Addendum, acting on its own account and for and on behalf of those of its Affiliates and customers (where applicable) that are the controllers of Personal Data,

(hereinafter the "**data exporter**");

and **Centercode, Inc.**

(hereinafter the "**data importer**");

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

[remainder of page intentionally left blank]

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Customer

Signatory Name: _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

Centercode, Inc.

Name: Luke Freiler

Position: Chief Executive Officer

Address: 23332 Mill Creek Drive, Suite 260, Laguna Hills, CA 92653

Signature: _____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Terms used in this Appendix 1 have the meaning given to them in the Data Processing Addendum to which these Standard Contractual Clauses have been appended.

Data exporter

The data exporter is the entity identified as "**Customer**" in the Data Processing Addendum.

Data importer

The data importer is **Centercode, Inc.**, a provider of Services under its Agreement with the data exporter, which involves processing personal data provided by, and pursuant to the instructions and directions of, the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Data subjects

The categories of data subjects whose personal data may be transferred in connection with the Services are determined and controlled by the data exporter in its sole discretion and may include (without limitation):

> customers and customer prospects of the data exporter; employees and contractors of the data exporter; participants in Alpha, Beta, or Field Tests performed by or on behalf of data exporter, and other end-users.

Categories of data

The categories of personal data are determined by the data exporter in its sole discretion and may include (without limitation):

> 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.

Special categories of data (if appropriate)

The special categories of personal data, if any, are determined by the data exporter in its sole discretion and may include the following (or if left blank, none):

_____

[insert if applicable]

Processing operations

The personal data transferred will be subject to the following basic Processing activities:

Processing activities in the performance of the Services as set forth in the Agreement. Customer instructs Centercode to Process personal data for the purpose of performing the Services in the country in which Centercode or its Sub-processors maintain facilities as necessary for the provision of the Services as identified in the Data Processing Addendum.

On behalf of the data exporter:

Customer

Signatory Name: _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

Centercode, Inc.

Name: Luke Freiler

Position: Chief Executive Officer

Address: 23332 Mill Creek Drive, Suite 260, Laguna Hills, CA 92653

Signature: 

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures implemented by the data importer are as described in the Data Processing Addendum.

On behalf of the data exporter:

Customer

Signatory Name: _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

Centercode, Inc.

Name: Luke Freiler

Position: Chief Executive Officer

Address: 23332 Mill Creek Drive, Suite 260, Laguna Hills, CA 92653

Signature: _____

Annex 3

Supplemental Data Protection Terms – Data Sharing Arrangement

For the avoidance of doubt, this Annex 3 shall only apply where Customer is acting as a Data Controller of Betabound EU Data pursuant to Section 3.1 of the Data Processing Addendum.

1.1 In connection with Services involving Data Subjects from Centercode's Betabound Community of test participants, where Centercode (in its capacity as a Data Controller) transfers to Customer or provides Customer with access to Betabound EU Data for Customer to Process, it does so for the purpose(s) specified in Appendix 1 to this Annex 3 (the "Purpose").

1.2 Each party shall comply with the Data Protection Legislation in carrying out their obligations with respect to the Betabound EU Data, including those under this Annex 3.

1.3 If Customer is no longer able to Process the Betabound EU Data in a manner that is consistent with this Annex 3, 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.

1.4 Centercode will not transfer any Betabound EU Data to Customer except as specifically contemplated by the terms of the Agreement, this Annex 3, and the Data Protection Legislation.

1.5 If required to do so by a Supervisory Authority, Customer acknowledges and agrees that Centercode may disclose the Data Processing Addendum, including this Annex 3, to such Supervisory Authority and that such disclosure will not constitute a breach of confidence.

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

1.7 Customer may only transfer the Betabound EU Data from a country within the EEA 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.

1.8 Notwithstanding termination of the Agreement for any reason, Customer shall continue to protect the Betabound EU Data it received prior to termination as a Data Controller to the standard required by this Annex 3, including the Data Protection Legislation 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 EU Data in its possession or control. This provision shall survive termination of the Agreement, the Data Processing Addendum, and this Annex 3.

1.9 Each party shall be responsible for responding to any request, correspondence, inquiry, or complaint made directly to it regarding its Processing of the Betabound EU Data, but shall inform the other (to the extent

implicated in the request) of the request and how it intends to respond, unless prohibited from doing so by applicable Data Protection Legislation.

1.10 Each party shall implement appropriate technical and organisational measures in accordance with Article 32 of the GDPR and the Data Protection Legislation to ensure the security of the Betabound EU Data and protect it against any unauthorized and unlawful Processing, and against a Security Incident.

1.11 If Customer discovers or is notified of any Security Incident relating to the Betabound EU 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 Data Protection Legislation. 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.

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

1.13 Customer shall ensure that subcontractors it appoints to Process the Betabound EU Data provide at least the same level of protection for the Betabound EU Data and the rights of Data Subjects as Customer provides under this Annex 3. Each such subcontractor must be subject to a written agreement that is compliant with the Data Protection Legislation and which imposes obligations at least as restrictive as those imposed on Customer under this Annex 3. Customer will remain fully responsible and liable to Centercode for the performance of those obligations by each subcontractors. Customer shall further ensure that any such subcontractors only Process the Betabound EU Data in accordance with Customer's instructions and those instructions are consistent with the Purpose.

1.14 Customer shall ensure the reliability of any person that it authorizes to Process the Betabound EU 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 EU Data who is not under such a duty of confidentiality. Customer shall ensure that all such authorized persons Process the Betabound EU Data only as permitted by this Annex 3 and the Data Protection Legislation.

APPENDIX 1 TO ANNEX 3
DATA SHARING

This Appendix 1 to Annex 3 forms part of the Data Processing Addendum and describes the Processing that Customer will perform as a Data Controller.

Purpose

The Purpose of the transfer of Betabound EU Data to Customer is to enable Customer to use the Betabound EU Data in connection with Customer's use of Services deliverables relating to its Alpha, Beta, or Field Testing of its product, service, or application.

Personal Data

Customer is Processing as a Data Controller the following categories of Betabound EU Data:

Data Subjects:

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

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, and video

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

Processing operations

processing activities in the use of Services and Service deliverables related to Customer's Alpha, Beta, or Field testing of its product, service, or application