Data Processing Addendum

Last Updated: December 22, 2023

This Data Processing Addendum ("DPA") forms part of and is incorporated by this reference to the Agreement described in the Order Form between Calibo and Customer. All capitalized terms not defined in this DPA shall have the meanings set forth in the Order Form.

1. Definitions.

"**Authorized Affiliate**" shall mean a Customer Affiliate who has not signed an Order Form pursuant to the Agreement but is either a Data Controller or Data Processor for the Personal Data processed by Calibo pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all foreign, federal, and state privacy and data protection laws applicable to the each party under the Agreement, including, but not limited to: (i) 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) ("**GDPR**"); (ii) the UK Data Protection Act 2018 ("**UK Data Protection Act**"); and (iii) state privacy and data protection laws such as (a) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations as amended by the California Privacy Rights Act (collectively, the "**CCPA**"); (b) Virginia's Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq.; (c) the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq.; (d) Connecticut's Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015; (e) the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.; and (f) other state data privacy or data protection laws modeled on any of the foregoing, each as may be in effect and applicable to the parties' Processing of Personal Data. (collectively, "**State Privacy Laws**").

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**Processing**" shall mean 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, and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Calibo's provision of the Calibo Services as described in the Agreement, including Processing initiated by Users in their use of the Calibo Services; and (ii) further documented, reasonable instructions from Customer agreed upon by the Parties.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as defined by applicable Data Protection Laws.

"**Service Provider**" means a person that Processes Personal Data on behalf of a business and that receives from or on behalf of the business consumer's Personal Information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the Personal Data that the Service Provider receives from, or on behalf of, the business with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the Service Provider may combine Personal Data to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of

> Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

“**Sub-processor**” means any other Data Processors engaged by a member of the Calibo to Process Customer Personal Data.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that Calibo Processes Personal Data on behalf of Customer as Data Processor in the course of providing the Calibo Services.

3. Roles and Scope of Processing.

3.1. Role of the Parties. As between Calibo and Customer, Calibo shall Process Personal Data only as a Data Processor (or Sub-Processor) acting on behalf of Customer and, with respect to CCPA, as a Service Provider in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller (such third-party, the “**Third-Party Controller**”) with respect to Customer Personal Data. To the extent any Usage Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Calibo is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2. Customer Instructions. Calibo will Process Personal Data only for the Purposes. Customer shall ensure its Processing instructions comply with applicable Data Protection Laws and that the Processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The Parties agree that the Agreement (including this DPA) sets out the exclusive and final instructions to Calibo for all Processing of Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions require the prior written agreement of Calibo. Calibo shall promptly notify Customer if, in Calibo’s reasonable opinion, such instruction violates Data Protection Laws. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

3.3. Customer Affiliates. Calibo’s obligations set forth in this DPA also extend to Authorized Affiliates, subject to the following conditions:

(a) Customer must exclusively communicate any additional Processing instructions requested pursuant to Section 3.2 directly to Calibo, including instructions from its Authorized Affiliates;

(b) Customer shall be responsible for Authorized Affiliates’ compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer’s obligations in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Calibo. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or other forms of complaints or proceedings against Calibo (“**Authorized Affiliate Claim**”): (i) Customer must bring such Authorized Affiliate Claim directly against Calibo on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including, but not limited to, any aggregate limitation of liability.

3.4. Processing of Personal Data. Each Party will comply with its respective obligations under Data Protection Laws. Customer agrees (i) it will use the Service in a manner designed to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing-up Customer Personal Data; and (ii) it has obtained all consents, permissions and/or rights necessary under Data Protection Laws for Calibo to lawfully Process Personal Data for the Purposes, including, without limitation, Customer’s sharing and/or receiving of Personal Data with third-parties via the Service.

3.5. Details of Data Processing.

(a) Subject Matter. The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Frequency and duration. Notwithstanding expiration or termination of the Agreement, Calibo will Process the Personal Data continuously and until deletion of all Personal Data as described in this DPA.

(c) Purpose. Calibo will Process the Personal Data only for the Purposes, as described in this DPA.

(d) Nature of the Processing. Calibo will perform Processing as needed for the Purposes, and to comply with Customer's Processing instructions as provided in accordance with the Agreement and this DPA.

(e) Retention Period. The period for which Personal Data will be retained and the criteria used to determine that period is determined by Customer during the term of the Agreement via Customer's use and configuration of the Service. Upon termination or expiration of the Agreement, Customer may retrieve or delete Personal Data as described in the Agreement, subject to applicable Law. Any Personal Data not deleted by Customer shall be deleted by Calibo promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" described in the Agreement.

(f) Categories of Data Subjects. The categories of Data Subjects to which Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);
(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or
(iii) Employees, agents, advisors, and freelancers of Customer (who are natural persons).

(g) Categories of Personal Data. The types of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);
(ii) Financial information (credit card details, account details, payment information);
(iii) Employment details (employer, job title, geographic location, area of responsibility); and/or
(iv) IT information (IP addresses, cookies data, location data).

(h) Special Categories of Personal Data (if applicable). Subject to any applicable restrictions and/or conditions in the Agreement or Documentation, Customer may also include 'special categories of personal data' or similarly sensitive Personal Data (as described or defined in Data Protection Laws) in Customer Personal Data, the extent of which is determined and controlled by Customer in its discretion, and which may include, but is not limited to Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.

4. Sub-Processing.

4.1. Authorized Sub-Processors. Customer provides Calibo with a general authorization to engage Sub-processors, subject to Section 4.3 (Changes to Sub-processors), as well as Calibo's list of Sub-processors that it may use from time to time listed at [www.calibo.com/legal] ("**Sub-processor Site**") as of the effective date of this DPA and members of the Calibo.

4.2. Sub-processor Obligations. Calibo shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Personal Data as Calibo's obligations under this DPA to the extent applicable to the services provided by the Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, Calibo shall provide Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Customer's obligations under Data Protection Laws.

4.3. Changes to Sub-processors. Calibo shall make available on its Sub-processor Site a mechanism to subscribe to notifications of new Sub-processors. Calibo shall provide such notification to those emails that have subscribed at least twenty-eight (28) days in advance of allowing the new Sub-processor to Process Personal Data (the "**Objection Period**"). During the Objection Period, objections (if any) to Calibo's appointment of the new Sub-processor must be provided to Calibo in writing and based on reasonable grounds. In such event, the Parties will discuss those objections in good faith with a view to achieving resolution. If it can be reasonably demonstrated to Calibo that the new Sub-processor is unable to Process Personal Data in compliance with the terms of this DPA and Calibo cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect to only those aspects which cannot be provided by Calibo without the use of the new Sub-processor by providing advance written notice to Calibo of such termination. Calibo will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of such termination.

5. Security.

5.1. Security Measures. Calibo shall implement and maintain appropriate technical and organizational security measures (see www.calibo.com/legal/toms) designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data.

5.2. Confidentiality of Processing. Calibo shall ensure that any person who is authorized by Calibo to Process Personal Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3. No Assessment of Personal Data by Calibo. Calibo shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for making an independent determination as to whether its use of the Service will meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

6.1. Upon written request and at no additional cost to Customer, Calibo shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Calibo's compliance with its obligations under this DPA in the form of the relevant audits or certifications listed in the Security Addendum, such as (i) ISO 27001 and 27017, and (ii) relevant audit reports (collectively, "**Reports**").

6.2. Customer may also send a written request for an audit of Calibo's applicable controls, including inspection of its facilities. Following receipt by Calibo of such request, Calibo and Customer shall mutually agree in advance on the details of the audit, including the reasonable start date, scope, and duration of, and security and confidentiality controls applicable to, any such audit. Calibo may charge a fee (rates shall be reasonable, considering the resources expended by Calibo) for any such audit. The Reports, audit, and any information arising therefrom shall be considered Calibo's Confidential Information and may only be shared with a third-party (including a Third-Party Controller) with Calibo's prior written agreement.

6.3. Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement or non-disclosure agreement with Calibo prior to any review of Reports or an audit of Calibo, and Calibo may object in writing to such Auditor, if in Calibo's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Calibo. Any such objection by Calibo will require Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of Reports or an audit shall be borne exclusively by the Auditor. For clarity, the exercise of audit rights under a Transfer Mechanism shall be as described in this Section 6 (Customer Audit Rights) and Customer agrees those rights are carried out on behalf of Customer and all relevant Third-Party Controllers, subject to the confidentiality and non-use restrictions of the Agreement.

7. Data Transfers.

7.1. Processing Locations. Calibo will only host Customer Data in the region(s) offered by Calibo and set forth on the Order Form in the Agreement with Customer. Customer is solely responsible to comply with all applicable Laws in the regions from which its Users access the Calibo Platform for any transfer or sharing of Personal Data by Customer or its Users. Calibo will not Process Personal Data from outside the tenant location set forth in the Order Form except as necessary to comply with applicable Laws or binding order of a governmental body.

7.2. Transfer Mechanisms.

7.2.1. Transfer Mechanisms and/or Contract Clauses Prescribed by Data Protection Laws. If Data Protection Laws have prescribed specific mechanisms for the transfer of Personal Data to Calibo and/or contract clauses for Processing of Personal Data by Calibo (collectively, a "**Transfer Mechanism**"), Calibo shall make such specific Transfer Mechanism available (to the extent generally supported by Calibo) at [www.calibo.com/legal] (the "**Transfer Mechanism Site**"). A Transfer Mechanism shall not apply and shall not be incorporated into this DPA if it is not applicable to (i) transfers from Customer to Calibo (including where no such transfer occurs), or (ii) Processing by Calibo of Customer Personal Data. If a listed Transfer Mechanism is, or becomes applicable under Data Protection Laws, it shall be deemed to be signed by the Parties and is incorporated into this DPA. Subject to Section 7.2.2 (Updates Regarding Transfer Mechanism Site) below, Calibo may only remove an applicable Transfer Mechanism if the Transfer Mechanism has ceased being valid under the Data Protection Law or Calibo is offering an alternative, then-currently valid Transfer Mechanism.

7.2.2. Updates Regarding Transfer Mechanism Site. Calibo shall notify Customer of changes to its Transfer Mechanisms by updating the Transfer Mechanism Site and posting a summary and date of the relevant changes.

8. Incident IssueResponse.

8.1. Incident IssueReporting. If Calibo becomes aware of a Incident Issue, Calibo shall notify Customer without undue delay, and in any case, where feasible, notify Customer within the applicable time period required under Data Protection Laws. Calibo's notification shall be sent to the Customer Representative identified in the Order Form. Calibo shall promptly take reasonable steps to contain, investigate, and mitigate any Incident Issue.

8.2. Incident Issue**Communications**. Calibo shall provide Customer timely information about the Incident Issue, including, but not limited to, the nature and consequences of the Incident Issue, the measures taken and/or proposed by Calibo to mitigate or contain the Incident Issue, the status of Calibo's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Calibo personnel may not have visibility to the content of Customer Personal Data, it is unlikely Calibo can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number, or categories of affected Data Subjects. Communications by or on behalf of Calibo with Customer in connection with a Incident Issueshall not be construed as an acknowledgment by Calibo of any fault or liability with respect to the Incident Issue.

9. Cooperation.

9.1. Data Subject Requests. Calibo shall promptly notify Customer if Calibo receives a request from a Data Subject that identifies Personal Data or otherwise identifies Customer, including where the Data Subject seeks to exercise any of its rights under applicable Data Protection Laws (collectively, "**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to Data Subject Requests and, subject to the next sentence, Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Personal Data within the Service using such controls or otherwise, Calibo shall (upon Customer's written request and considering the nature of Calibo's Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

9.2. Data Protection Impact Assessments. Calibo shall provide reasonably requested information regarding the Service to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

9.3. Government & Law Enforcement Inquiries. If Calibo receives a demand to retain, disclose, or otherwise Process Personal Data from law enforcement or any other government and/or public authority ("Third-Party Demand"), then Calibo shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Calibo can provide information to such third-party to the extent reasonably necessary to redirect the Third-Party Demand to Customer. If Calibo cannot redirect the Third-Party Demand to Customer, then Calibo shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy. This section does not diminish Calibo's obligations under any applicable Transfer Mechanisms with respect to access by public authorities.

10. Relationship with the Agreement.

10.1. Entire Agreement. The Parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Calibo and Customer may have previously entered into in connection with the Service. Calibo may update this DPA from time to time, with such updated version posted to [www.calibo.com/legal], or a successor website designated by Calibo; provided, however, that no such update shall materially diminish the privacy or security of Customer's Personal Data.

10.2. Conflicting Terms. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Personal Data comprised of patient, medical or other protected health information regulated by HIPAA, if there is any conflict between this DPA and a BAA between Customer and Calibo, then the BAA shall prevail solely with respect to such Customer Personal Data.

10.3. Limitations on Liability. Notwithstanding anything to the contrary in the Agreement or this DPA, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of, or relating to this DPA, the Transfer Mechanisms, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the Parties' obligations under the Agreement, each Party agrees that any regulatory penalties incurred by one Party (the "**Incurring Party**") in relation to the Personal Data that arise as a result of, or in connection with, the other Party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other Party under the Agreement.

10.4. Rights or Remedies. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the Transfer Mechanisms).

10.5. Governing Law. This DPA will be governed by and construed in accordance with governing Law and jurisdiction provisions in the Agreement.