THRIVE DATA PROTECTION ADDENDUM

The undersigned party agreeing to these terms ("***Client***") has entered into a Standard Terms and Conditions Agreement (as amended from time to time, the "***Agreement***") with Thrive TRM LLC ("***Thrive***"), under which Thrive has agreed to provide the certain services described therein ("***Services***") to Client.

This Data Protection Addendum, including its appendices (the "***Addendum***"), supplements and forms part of the Agreement.

1. Definitions

For purposes of this Addendum, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this Addendum have the meanings given in the Agreement.

1.1 **Account Data** means the Personal Data of Client employees, personnel, contractors, business contacts, and/or agents that relates to Client's business relationship with Thrive, including without limitation the names or contact information of Authorized Users, and contact and billing information of individuals that Client has associated with its account.

1.2 **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.3 **Applicable Data Protection Laws** means European Data Protection Laws and the CCPA, in each case, to the extent applicable to the relevant Personal Data or processing thereof under the Agreement.

1.4 **CCPA** means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder, in each case, as amended from time to time.

1.5 **Client Personal Data** means the Personal Data included in Submitted Data. For purposes of this Addendum, Client Personal Data does not include Account Data, Usage Data or Thrive Data.

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

1.7 **EU** means the European Union.

1.8 **European Data Protection Laws** means the GDPR for the EU and its Member States, the Switzerland Federal Act on Data Protection ("***FADP***"), and the United Kingdom Data Protection Act 2018 (the "***UK GDPR***"), in each case, to the extent it applies to the relevant Personal Data or processing thereof under the Agreement.

1.9 **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

1.10 **Information Security Incident** means a breach of Thrive's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data in Thrive's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Client Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.11 **Personal Data** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

1.12 **Security Measures** has the meaning given in Section 4.1 (Thrive's Security Measures).

1.13 **Standard Contractual Clauses** means the mandatory provisions of the standard contractual clauses for the transfer of Personal Data to any country that does not have an adequate level of data protection to permit the transfer of Personal Data to (pursuant to a decision of the relevant supervisory authority) ("***Third Country***"). For the EU, the Standard Contractual Clauses shall be

the form set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.14 **Subprocessors** means third parties authorized under this Addendum to process Personal Data in relation to the Service.

1.15 **Third Party Subprocessors** has the meaning given in Section 5 (Subprocessors) of Annex 1.

1.16 **Usage Data** means the statistical and analytical data related to Thrive's provision of the Services, including but not limited to meta data, log data and IP address. Usage Data also includes information relating to how Authorized Users are using and interacting with the Services (e.g., the number of concurrent users in the system, page load statistics, upload statistics).

1.17 The terms **controller**, **data subject**, **processing**, **processor** and **supervisory authority** as used in this Addendum have the meanings given in Applicable Data Protection Laws. For purposes of this Addendum "**controller**" shall include "**business**" as defined in the CCPA, "**processor**" shall include "**service provider**" as defined in the CCPA and "**data subject**" shall include "**consumers**" as defined in the CCPA. The terms **sell** and **share** shall have the meanings given in the CCPA.

2. Duration and Scope of Addendum

2.1 This Addendum will, notwithstanding the expiration of the Agreement, remain in effect until, and automatically expire upon, Thrive's deletion of all Client Personal Data.

2.2 Annex 1 (EU Annex) to this Addendum applies to Client Personal Data or the processing thereof subject to European Data Protection Laws. Annex 2 (California Annex) to this Addendum, applies to Client Personal Data or the processing thereof subject to the CCPA.

3. Client Instructions

The parties agree and acknowledge that with respect to the processing of Client Personal Data in connection with the Agreement and provision of the Services, Thrive is a processor and Client is a controller of Client Personal Data. Thrive will process Client Personal Data only in accordance with Client's instructions. By entering into this Addendum, Client instructs Thrive to process Client Personal Data to provide the Services. Client acknowledges and agrees that such instruction authorizes Thrive to process Client Personal Data (a) to perform its obligations and exercise its rights under the Agreement; (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; (c) pursuant to any other written instructions given by Client and acknowledged in writing by Thrive as constituting instructions for purposes of this Addendum; and (d) as reasonably necessary for the proper management and administration of Thrive's business.

4. Security

4.1 Thrive Security Measures. Thrive will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as set forth in Annex 3 (the "***Security Measures***").

4.2 Information Security Incidents. If Thrive becomes aware of an Information Security Incident, Thrive will (a) notify Client of the Information Security Incident within seventy-two (72) hours after becoming aware of the Information Security Incident and (b) take reasonable steps to identify the cause of such Information Security Incident, minimize harm and prevent a recurrence. Notifications made pursuant to this Section 4.2 will describe, to the extent known, details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Thrive recommends Client take to address the Information Security Incident. Thrive's notification of or response to an Information Security Incident under this Section 4.2 will not be construed as an acknowledgement by Thrive of any fault or liability with respect to the Information Security Incident. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory and/or regulatory authorities. Other than agreeing on the content of related public statements or required notices, Client is solely responsible for

complying with breach notification laws applicable to Client and fulfilling any breach notification obligations related to any Information Security Incident(s).

4.3 Client's Security Responsibilities and Assessment

4.3.1 Client's Security Responsibilities. Client agrees that, without limitation of Thrive's obligations under Section 4.1 (Thrive Security Measures) and Section 4.2 (Information Security Incidents), Client is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of Client Personal Data; (b) securing the account authentication credentials, systems and devices Client uses to access the Service; (c) securing Client's systems and devices that Thrive uses to provide the Service; and (d) backing up Client Personal Data.

4.3.2 Client's Security Assessment. Client is solely responsible for evaluating for itself whether the Service, the Security Measures and Thrive's commitments under this Addendum will meet Client's needs, including with respect to any security obligations of Client under Applicable Data Protection Laws or other laws. Client acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Client Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Thrive provide a level of security appropriate to the risk in respect of the Client Personal Data.

5. Data Subject Rights

5.1 Client's Responsibility for Requests. If Thrive receives any request from a data subject in relation to Client Personal Data, Thrive will advise the data subject to submit the request to Client and Client will be responsible for responding to any such request.

5.2 Thrive's Data Subject Request Assistance. Thrive will (taking into account the nature of the processing of Client Personal Data) provide Client with self-service functionality through the Service or other reasonable assistance as necessary for Client to perform its obligation under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws, including if applicable, Client's obligation to respond to requests for exercising the data subject's rights set out in the CCPA and/or Chapter III of the GDPR. Client shall reimburse Thrive for any such assistance, beyond providing self-service features included as part of the Service, at Thrive's then-current professional services rates, which shall be made available to Client upon request.

6. Client Responsibilities

Client represents and warrants to Thrive that (a) Client's instructions to Thrive for processing Client Personal Data shall comply with Applicable Data Protection Laws; (b) Client has established or ensured that another party has established a legal basis for Thrive's processing of Client Personal Data contemplated by this Addendum; (c) all notices have been given to, and consents and rights have been obtained from, the relevant data subjects and any other party as may be required by Applicable Data Protection Laws and any other laws for such processing; and (d) Client Personal Data does not and will not contain any protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA), any sensitive Personal Data, such as biometric information or any payment card information subject to the Payment Card Industry Data Security Standard. Client shall have sole responsibility for the accuracy, quality, and legality of Client Personal Data and the means by which the Client acquired Client Personal Data. Client specifically acknowledges that its use of the Services will not violate the rights of any data subject that has requested deletion of or opt out of the sale, sharing or other disclosures of Client Personal Data, to the extent applicable under Applicable Data Protection Laws.

7. Reviews and Audits of Compliance

7.1 Thrive evaluates, tests, and monitors the effectiveness of Thrive's information security program and adjusts and/or updates Thrive's information security program as reasonably warranted by the results of such evaluation, testing, and monitoring. Thrive, from time to time, may conduct an assessment of the implementation and maintenance of Thrive's information security program and its related compliance with Applicable Data Protection Laws ("***Audit***"). Upon Client's reasonable written request, Thrive shall provide a summary of the findings and observations of

its then-current Audit ("***Audit Report***"); provided, however, that Client agrees that any such Audit Report is the confidential information of Thrive and Client will not disclose them to third parties except for Client's legal counsel and consultants bound by obligations of confidentiality.

7.2 If the Audit Report is insufficient to demonstrate Thrive's compliance with this Addendum as required under Applicable Data Protection Laws, including where mandated by Client's supervisory authority, Client may audit Thrive's compliance with its obligations under this Addendum up to once per year and on such other occasions as may be required by Applicable Data Protection Laws, including where mandated by Client's supervisory authority. Thrive will reasonably contribute to such audits by providing Client or Client's supervisory authority with the information and assistance reasonably necessary to conduct the audit.

7.3 If a third party is to conduct the audit, Thrive may object to the auditor if the auditor is, in Thrive's reasonable opinion, not independent, a competitor of Thrive, or otherwise manifestly unsuitable. Such objection by Thrive will require Client to appoint another auditor or conduct the audit itself.

7.4 To request an audit, Client must submit a detailed proposed audit plan to Thrive at least thirty (30) days in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Thrive will review the proposed audit plan and provide Client with any concerns or questions (for example, any request for information that could compromise Thrive security, privacy, employment or other relevant policies). In any event, the audit shall be limited in scope to Thrive's processing of Client Personal Data only. Thrive will work cooperatively with Client to agree on a final audit plan. Nothing in this Section 7 shall require Thrive to breach any duties of confidentiality.

7.5 The audit must be conducted during regular business hours, subject to the agreed final audit plan and Thrive's safety, security or other relevant policies, and may not unreasonably interfere with Thrive business activities.

7.6 Client will promptly notify Thrive in writing of any non-compliance discovered during the course of an audit and provide Thrive any audit reports generated in connection with any audit under this Section 7, unless prohibited by Applicable Data Protection Laws or otherwise instructed by a supervisory authority. Client may use the audit reports only for the purposes of meeting Client's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum.

7.7 Any audits are at Client's expense. Client shall reimburse Thrive for any time expended by Thrive or its Subprocessors in connection with any audits or inspections under this Section 7 at Thrive's then-current professional services rates, which shall be made available to Client upon request. Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit. Nothing in this Addendum shall be construed to require Thrive to furnish more information about its Subprocessors in a connection with such audits than such Subprocessors make generally available to their customers.

8. Account Data and Usage Data

Client acknowledges and agrees that Thrive may create and derive from processing Client Personal Data under the Agreement anonymized and/or aggregated data that does not identify Client or any natural person, and use, disclose, publicize, sell and/or share with third parties such data to develop and enhance Thrive's products and services generally and for its other lawful business purposes. The parties agree that with regard to the processing of Account Data and Usage Data, Thrive is an independent controller of such data under Applicable Data Protection Laws. Thrive will comply with its obligations as controller for Account Data and Usage Data and process Account Data and Usage Data as a controller for its business purposes, including but not limited to: (a) manage and administer the relationship with Client; (b) carry out Thrive's internal business operations, such as and without limitation, billing and accounting; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) provide support services; (e) comply with Thrive's legal or regulatory obligations; (f) exercise its rights and

carry out its obligations under the Agreement; (g) improve and troubleshoot the Service; (h) develop and enhance Thrive's products and/or services; and (i) as otherwise permitted under Applicable Data Protection Laws, this Addendum, the Agreement, and Thrive's privacy policy located at https://thrivetrm.com/privacy-policy/.

9. Legally Required Disclosures.

Thrive may disclose Client Personal Data and any other information about Client to government or law enforcement officials or private parties if, in Thrive's reasonable discretion, Thrive believes it is necessary or appropriate in order to respond to legal requests, demands, and orders, including subpoena, judicial, administrative, or arbitral order of an executive or administrative agency, regulatory agency, supervisory authority or other governmental authority, to protect the safety, property, or rights of Thrive or of any third party, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with applicable law. Except as otherwise required by applicable law, Thrive will notify Client of any legal requests, demands, and orders that Thrive receives, and that relate to the processing of Client Personal Data.

10. Data Deletion

Upon termination of Client's access to the Service, Thrive shall delete all Client Personal Data from Thrive's systems as soon as reasonably practicable (and in no event later than thirty (30) days after termination), unless applicable law requires otherwise or where Thrive has archived such Client Personal Data on back-up systems, which will be deleted in accordance with Thrive's standard data retention policies and procedures. In the event Thrive retains Client Personal Data after termination of Client's access to the Service, Thrive shall continue to comply with its privacy and data security obligations under this Addendum until it is no longer in possession of Client Personal Data.

11. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Thrive to Client may be given (a) in accordance with any notice clause of the Agreement; (b) to Thrive's primary points of contact with Client; or (c) to any email provided by Client for the purpose of providing it with Service-related communications or alerts. Client is solely responsible for ensuring that such email addresses are valid.

12. Effect of These Terms

Except as expressly modified by the Addendum, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this Addendum and the other terms of the Agreement, this Addendum will govern. This Addendum replaces all other privacy, security or other data protection terms of the Agreement. Any liabilities arising in respect of this Addendum are subject to the limitations of liability under the Agreement.

In witness whereof and intending to be legally bound, the parties through their authorized representatives hereby accept and agree to this Addendum:

CLIENT	**THRIVE**
Client full corporate name:	Thrive TRM LLC
_____	
By: _____	By: _____
Name:	Name: Brandt Nelson
Title:	Title: VP of Sales
Date:	Date:

Annex 1

EU Annex

1. Processing of Data

1.1 Subject Matter and Details of Processing. The parties acknowledge and agree that (a) the subject matter of the processing under the Agreement is Thrive's provision of the Service; (b) the duration of the processing is from Thrive's receipt of Client Personal Data until deletion of all Client Personal Data by Thrive in accordance with the Agreement; (c) the nature and purpose of the processing is to provide the Service; (d) the data subjects to whom the processing pertains are Client's employees and other personnel, or candidates for employment by Client; and (e) the categories of Client Personal Data are contact details, workplace communications and other information processed by workplace information systems about such data subjects.

1.2 Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (a) Thrive is a processor of Client Personal Data under European Data Protection Laws; (b) Client is a controller of Client Personal Data under European Data Protection Laws; and (c) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the processing of Client Personal Data.

1.3 Thrive's Compliance with Instructions. Thrive will only process Client Personal Data in accordance with Client's instructions described in Section 3 (Client Instructions) of the Addendum unless European Data Protection Laws require otherwise, in which case Thrive will notify Client (unless that law prohibits Thrive from doing so on important grounds of public interest).

2. Data Security

2.1 Thrive Security Measures, Controls and Assistance

2.1.1 Thrive Security Assistance. Thrive will (taking into account the nature of the processing of Client Personal Data and the information available to Thrive) provide Client with reasonable assistance necessary for Client to comply with its obligations in respect of Client Personal Data under European Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 4.2 (Information Security Incidents) of the Addendum; and (c) complying with this Annex 1.

2.1.2 Security Compliance by Thrive Staff. Thrive will grant access to Client Personal Data only to Thrive personnel who need such access for the scope of their job duties, and are subject to appropriate confidentiality arrangements.

3. Impact Assessments and Consultations

Thrive will (taking into account the nature of the processing and the information available to Thrive) reasonably assist Client in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Thrive's information security program and the Security Measures applied in connection therewith; and (b) providing the other information contained in the Agreement including this Addendum.

4. Data Transfers

4.1 Data Processing Facilities. Thrive may, subject to Section 4.2 to this Annex 1 (Transfers out of the EEA), store and process Client Personal Data in the United States or anywhere Thrive or its Subprocessors maintains facilities.

4.2 Transfers out of the EEA. If Client transfers Client Personal Data out of the EEA to Thrive in a Third Country, such transfer will be governed by the Standard Contractual Clauses, the terms of which are hereby incorporated into this Addendum. In furtherance of the foregoing, the parties agree that:

4.2.1 for purposes of the Standard Contractual Clauses, Module 2 will apply.

4.2.2 for purposes of the Standard Contractual Clauses, (a) Client will act as the data exporter and (b) Thrive will act as the data importer;

4.2.3 for purposes of Annex 1, Part B, to the Standard Contractual Clauses, the categories of data subjects, data, and the processing operations shall be as set out in Section 1.1 to this Annex 1 (Subject Matter and Details of Processing);

4.2.4 for purposes of Annex 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures;

4.2.5 upon data exporter's request under the Standard Contractual Clauses, data importer will provide copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to the Standard Contractual Clauses. Data importer may remove or redact all commercial information or clauses unrelated to the Standard Contractual Clauses or their equivalent beforehand;

4.2.6 the audits described in the Standard Contractual Clauses shall be performed in accordance with Section 7 of the Addendum (Reviews and Audits of Compliance);

4.2.7 Client's authorizations in Section 5 of this Annex 1 (Subprocessors) will constitute Client's prior written consent to the subcontracting by Thrive of the processing of Client Personal Data if such consent is required under Clause 9(a) of the Standard Contractual Clauses;

4.2.8 In Clause 7 of the Standard Contractual Clauses, the optional docking clause will not apply;

4.2.9 In Clause 9 of the Standard Contractual Clauses, Option 2 will apply, and the requirements for prior notice of Subprocessor changes shall be as set out in Section 5 of this Annex 1 (Subprocessors);

4.2.10 In Clause 11 of the Standard Contractual Clauses, the optional language shall not apply;

4.2.11 certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Client's written request;

4.2.12 In Clause 17 of the Standard Contractual Clauses, Option 1 will apply;

4.2.13 In Clause 18(b) of the Standard Contractual Clauses, disputes shall be resolved before the courts of the jurisdiction governing the Agreement or, if that jurisdiction is not an EU Member State, then the courts in the jurisdiction associated with Client. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall correspond to the country of the governing law; and

4.2.14 notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA (e.g., US-E.U. Data Privacy Framework, binding corporate rules) applies to the transfer.

4.3 Transfers out of the UK. Where Client Personal Data protected by UK GDPR is transferred outside the United Kingdom to a Third Country, the Standard Contractual Clauses UK Addendum (*i.e.*, the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner under S119A(1) of the Data Protection Act 2018), shall apply as follows:

4.3.1 The EU Standard Contractual Clauses, completed as set out in Section 4.2 of this Annex 1 (Transfers out of the EEA) above, shall also apply to transfers of such Client Personal Data;

4.3.2 The Appendix Information (as defined in the Standard Contractual Clauses UK Addendum) shall be deemed completed with the relevant information set out in Section

1.1 to this Annex 1 (Subject Matter and Details of Processing), the Security Measures, and Section 5 of this Annex 1 (Subprocessors); and

4.3.3 The Standard Contractual Clauses UK Addendum shall be deemed executed between Client and Thrive, and the Standard Contractual Clauses shall be deemed amended as specified by the UK Addendum in respect of the transfer of Client Personal Data.

4.4 Transfers out of Switzerland. Where Client Personal Data is transferred outside Switzerland to a Third Country and such data transfer is governed by FADP, the Standard Contractual Clauses, completed as set out in Section 4.2 of this Annex 1 (Transfers out of the EEA) above, shall apply to such data transfers, with the following exceptions:

4.4.1 Without prejudice to Clause 13 (a) the competent supervisory authority in respect of the data transfer governed by FADP, pursuant to Annex I.C of the EU Standard Contractual Clauses shall be the Swiss Federal Data Protection and Information Commissioner;

4.4.2 In Clause 17, the governing law shall be the laws of Switzerland;

4.4.3 In Clause 18(c), the competent courts shall be the courts of Zurich, Switzerland;

4.4.4 Any references to "Member State(s)" in the Standard Contractual Clauses shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU Standard Contractual Clauses in Switzerland;

4.4.5 Any references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the Standard Contractual Clauses shall be complemented with references to the FADP (as amended or replaced).

5. Subprocessors

5.1 Consent to Subprocessor Engagement. Client specifically authorizes the engagement of Thrive's Affiliates as Subprocessors. In addition, Client generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**").

5.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at https://thrivetrm.com/thrive-trm-sub-processors/ (as may be updated by Thrive from time to time in accordance with this Annex 1).

5.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Thrive will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this Addendum with respect to Client Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Thrive shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

5.4 Opportunity to Object to Subprocessor Changes. When any new Third Party Subprocessor is engaged during the term of the Agreement, Thrive will notify Client of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the website listed in Section 5.2 of this Annex 1 (Information about Subprocessors). If Client objects to such engagement in a written notice to Thrive within fifteen (15) days of being informed thereof on reasonable grounds relating to the protection of Client Personal Data, Client and Thrive will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Client may, as its sole and exclusive remedy, terminate the Agreement with respect only to those Services which cannot be provided by Thrive without the use of the objected-to new Subprocessor by providing written notice to Thrive.

Annex 2

California Annex

1. Thrive shall not (a) sell or share any Client Personal Data that constitutes "personal information" under the CCPA ("**CA Personal Information**"); (b) retain, use or disclose any CA Personal Information for any purpose other than for the specific purpose of providing the Services or as otherwise permitted by the CCPA, including retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in the CCPA) other than provision of the Services; (c) retain, use or disclose the CA Personal Information outside of the direct business relationship between Thrive and Client or as otherwise permitted by the CCPA; or (d) combine CA Personal Information with other Personal Data collected by Thrive and its Affiliates from sources other than Client. Thrive hereby certifies that it understands its obligations under this Section 1 and will comply with them.

2. Provision of the Services encompasses the processing authorized by Client's instructions described in Section 3 of the Addendum (Client Instructions).

3. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Thrive's access to CA Personal Information or any other Client Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

4. Thrive shall comply with its obligations under CCPA as a service provider and shall, without undue delay, notify Client if Thrive makes a determination that it can no longer meet its obligations under the CCPA.

5. Thrive shall contractually require its Subprocessors to agree to restrictions, conditions, and requirements that, taken as a whole, are at least as protective of CA Personal Information as those that apply to Thrive under the Addendum and this Annex 2 (California Annex).

Annex 3

Security Measures

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Thrive's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Thrive's organization, monitoring and maintaining compliance with Thrive's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
3. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:
    a. transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or
    b. at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).
5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Thrive passwords that are assigned to its employees: (i) be at least eight (8) characters in length; (ii) not be stored in readable format on Thrive's computer systems; (iii) must be changed every ninety (90) days; (iv) must have defined complexity; (v) must have a history threshold to prevent reuse of recent passwords; and (vi) newly issued passwords must be changed after first use.
6. Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Thrive facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
7. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Thrive's technology and information assets.
8. Incident / problem management procedures designed to allow Thrive to investigate, respond to, mitigate and notify of events related to Thrive's technology and information assets.
9. Network security controls that provide for the use of enterprise firewalls, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
10. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
11. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Thrive may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.