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 **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.

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

1.3 **CPRA** means the California Privacy Rights Act of 2020 and any regulations promulgated thereunder, in each case, as amended from time to time.

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

1.5 **EU** means the European Union.

1.6 **European Data Protection Laws** means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent it applies to the relevant Personal Data or processing thereof under the Agreement.

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

1.8 **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, 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 Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.9 **Personal Data** means the personal data and personal information (as defined by Applicable Data Protection Laws) that Thrive processes for Client pursuant to the Agreement.

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

1.11 **Standard Contractual Clauses** means the mandatory provisions of the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set out by European Commission Decision 2021/914/EU, or any successor documents or data transfer schemes.

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

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

1.14 **UK International Data Transfer Agreement** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022**.**

1.15 **VCDPA** means the Virginia Consumer Data Protection Act of 2021 and any regulations promulgated thereunder, in each case, as amended from time to time.

1.16 The terms **controller**, **data subject**, **processing**, **processor** and **supervisory authority** as used in this Addendum have the meanings given in the Applicable Data Protection Laws.

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 Personal Data.

2.2 Annex 1 (EU Annex) to this Addendum applies to Personal Data or the processing thereof subject to European Data Protection Laws. Annex 2 (United States Annex) to this Addendum, applies to Personal Data or the processing thereof subject to the CPRA or VCDPA.

3. Client Instructions

Thrive will process Personal Data only in accordance with Client's instructions. By entering into this Addendum, Client instructs Thrive to process Personal Data to provide the Services. Client acknowledges and agrees that such instruction authorizes Thrive to process Personal Data (a) to perform its obligations and exercise its rights under the Agreement; (b) 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 described 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 without undue delay 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 possible, 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.

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 the 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 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 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 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 the data subject's 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 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. 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 has established or ensured that another party has established a legal basis for Thrive's processing of Personal Data contemplated by this Addendum; (b) 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 (c) Personal Data does not and will not contain any protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA), any biometric information, or any payment card information subject to the Payment Card Industry Data Security Standard.

7. Analytics

As part of the Services, Client acknowledges and agrees that: (a) Thrive may create and derive from processing Personal Data under the Agreement anonymized and/or aggregated data that does not identify Client or any natural person; and (b) Thrive owns all rights and interest in and to such data, and may use, publicize or share with third parties such data to improve Thrive's products and services and for its other lawful business purposes.

8. 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.

9. 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.

Accepted and agreed to by the authorized representative of each party:

CLIENT	**THRIVE**
Client full corporate name:	Thrive TRM LLC
_____	
By: _____	By: _____
Name:	Name:
Title:	Title:
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 Personal Data until deletion of all 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 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 that Personal Data under European Data Protection Laws; (b) Client is a controller of that 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 that Personal Data.

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

1.4 Data Deletion. Upon termination of Client's access to the Service, Client instructs Thrive to delete all Personal Data from Thrive's systems as soon as reasonably practicable, unless European Data Protection Laws requires otherwise.

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 Personal Data and the information available to Thrive) provide Client with reasonable assistance necessary for Client to comply with its obligations in respect of 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 Personal Data only to Thrive personnel who need such access for the scope of their job duties, and are subject to appropriate confidentiality arrangements.

2.2 Reviews and Audits of Compliance

2.2.1 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 European Data Protection Laws, including where mandated by Client's supervisory authority. Thrive will contribute to such audits by providing Client or Client's supervisory authority with the information and assistance reasonably necessary to conduct the audit.

2.2.2 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.

2.2.3 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). Thrive will work cooperatively with Client to agree on a final audit plan. Nothing in this Section 2.2 shall require Thrive to breach any duties of confidentiality.

2.2.4 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.

2.2.5 Client will promptly notify Thrive 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 2.2, unless prohibited by European 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.

2.2.6 Any audits are at Client's expense. Client shall reimburse Thrive for any time expended by Thrive or its Third Party Subprocessors in connection with any audits or inspections under this Section 2.2 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 Third Party Subprocessors in a connection with such audits than such Third Party Subprocessors make generally available to their customers.

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 (Transfers out of the EEA), store and process Personal Data in the United States or anywhere Thrive or its Subprocessors maintains facilities.

4.2 Transfers out of the UK or EEA. If Client transfers Personal Data out of the UK or EEA to Thrive in a country not deemed by the European Commission to have adequate data protection, and if no other solution enables the lawful transfer of such Personal Data in accordance with European Data Protection Law, then such transfer will be governed by either the Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the parties agree that:

4.2.1 for purposes of Annex I, Part A, to the Standard Contractual Clauses and Table 1 of the UK International Data Transfer Agreement, (a) Client will act as the data exporter, (b) Thrive will act as the data importer, and (c) the contact details for each party will be as set forth in the Agreement;

4.2.2 for purposes of Annex I, Part B, to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the processing operations shall be as set out in Section 1.1 to this Annex 1;

4.2.3 for purposes of Annex I, Part C, to the Standard Contractual Clauses, the competent supervisory authority will be the Irish Data Protection Commission;

4.2.4 in Clause 7 of the Standard Contractual Clauses, the optional docking clause will not apply;

4.2.5 in Clause 8.9 of the Standard Contractual Clauses, audits shall be performed in accordance with Section 2.2 of this Annex 1;

4.2.6 in Clause 9 of the Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of subprocessor changes will be as set forth in Section 5.4 of this Annex 1;

4.2.7 in Clause 11 of the Standard Contractual Clauses, the optional language will not apply;

4.2.8 in Clause 17 of the Standard Contractual Clauses, Option 1 will apply and the law will be Irish law;

4.2.9 in Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before courts in Ireland;

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

4.2.11 upon data exporter's request under the Standard Contractual Clauses, data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to Clause 9(c) of the Standard Contractual Clauses, and that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand;

4.2.12 in accordance with Section 2.2 of this Annex 1;

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

4.2.14 in Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located earlier in this Section 4.2;

4.2.15 in Table 3 of the UK International Data Transfer Agreement, the list of parties is located in Section 4.2.1 of this Annex 1, the description of the transfer is set forth in Section 4.2.2 of this Annex 1, the technical and organiziation measures are the Security Measures, and the list of sub-processors is located in Section 5.2 of this Annex 1; and

4.2.16 in Table 4 of the UK International Data Transfer Agreement, both the importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

4.3 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. binding corporate rules) applies to the transfer.

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 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 (Information about Subprocessors). If Client objects to such engagement in a written notice to Thrive within 15 days of being informed thereof on reasonable grounds relating to the protection of 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 and cancel the Service by providing written notice to Thrive.

Annex 2

United States Annex

1. Thrive shall not retain, use, or disclose any Personal Data that constitutes "personal information" under the CPRA or VCDPA ("**US Personal Information**") for any purpose other than for the specific purpose of providing the Services, or as otherwise permitted by CPRA or VCDPA, including retaining, using, or disclosing the US Personal Information for a commercial purpose (as defined in CPRA) other than providing the Services.

2. Thrive shall not (a) sell or share any US Personal Information; (b) retain, use or disclose any US Personal Information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the US Personal Information for a commercial purpose (as defined in the CPRA) other than provision of the Services or as otherwise permitted by the CPRA;(c) retain, use or disclose the US Personal Information outside of the direct business relationship between Thrive and Client. Thrive hereby certifies that it understands its obligations under this Section 2 and will comply with them; or (d) combining the US Personal Information which Thrive receives from or on behalf of Client, with US Personal Information which Thrive receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that Thrive may combine US Personal Information to perform any business purpose as defined in CPRA or VCDPA.

3. Thrive acknowledges that US Personal Information is disclosed to it by Client only for the limited and specific purposes set forth herein. Client may take reasonable and appropriate steps to help ensure that Thrive uses the US Personal Information in a manner consistent with Thrive's obligations herein. Such steps are limited to the steps described in Sections 2 and 3 of Annex 1 of this DPA, or as otherwise agreed by the parties in writing. Thrive will notify Client if Thrive makes a determination that it can no longer comply with its obligations under CPRA or VCDPA. Client may, upon at least ten (10) days' prior written notice to Thrive, take reasonable and appropriate steps to stop and remediate Thrive's unauthorized use of US Personal Information. Such steps are limited to the termination right set forth in Agreement (including the post-termination deletion obligations therein).

4. In furtherance of complying with the VCPDA: (a) the instructions for processing US Personal Information, the nature and purpose of processing, the type of data subject to processing, and the duration of processing are set forth in Section 1 of Annex 1 of this DPA; (b) Thrive shall ensure that each person processing US Personal Information is subject to a duty of confidentiality with respect to the US Personal Information; (c) Thrive's obligations to delete or return all US Personal Information are as set forth in Section 7.3 of the Agreement; (d) Thrive shall make available to Client all information in its possession necessary to demonstrate compliance with the obligations in this chapter, which is limited to taking the steps described in Sections 2 and 3 of Annex 1 of this DPA; and (e) Thrive shall allow, and contribute to, reasonable audits and inspections by Client or the Client's designated auditor, or alternatively, may arrange for a qualified and independent auditor to conduct an audit of Thrive's policies and technical and organizational measures in support of the obligations under this DPA, using an appropriate and accepted control standard or framework and audit procedure for such audits, each as further described in Sections 2 and 3 of Annex 1 of this DPA.

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

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

Annex 3

Security Measures

As from the Addendum Effective Date, Thrive will implement and maintain the Security Measures set out in this Annex 3.

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; must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) 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 design 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.