Updated: June 4, 2024

OATS DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is a part of, and shall be read together with, any Contract Documents (defined in Exhibit A). The DPA and Contract Documents collectively form the entire and exclusive agreement between Parties (the "Agreement").

WHEREAS:

OATS is a 501(c)(3) tax-exempt, nonprofit organization that provides resources and services (collectively known as "Senior Planet") to adults aged 60 and older ("seniors") which are designed to produce positive outcomes related to seniors' social connection, health and wellness, civic participation, economic security, creativity and lifelong learning; and

OATS has developed the Senior Planet licensing program to expand its reach in additional communities; and

OATS has developed and owns the rights and title to certain intellectual property described in the Agreement ("Licensed IP") that OATS uses in connection with its Senior Planet programs; and

Licensee provides programming for seniors and desires to license the Licensed IP from OATS to offer Senior Planet licensed programming to its clients; and

In furtherance of OATS' objective to expand its reach and help seniors access technology and use it to enhance their lives, OATS is willing to grant a license to Licensee subject to the terms and conditions of the Agreement; and

The Agreement includes Quality Assurance Requirements that contemplate Licensee's Processing of Personal Data that is governed by the provisions of this DPA.

IT IS AGREED AS FOLLOWS:

1. **DEFINITIONS**
   Definitions are set forth in Exhibit A to this DPA. Where a capitalized term is used but not otherwise defined in this DPA, it shall have the meaning ascribed to it elsewhere in the Agreement.

2. **DPA SCOPE/APPLICABILITY**
   Where no Personal Data is processed by Licensee in connection with the Agreement, only Sections 1, 2, 6 – 10, and Exhibit A apply to the Licensee.

3. **OWNERSHIP**
   Each Party hereby acknowledges and agrees that, as between Licensee and OATS, OATS owns all rights, title, and interest in and to the Personal Data that is Processed by Licensee on behalf of OATS pursuant to the Agreement. Further, as between Licensee and OATS, OATS is the Controller and

Business and Licensee is the Processor and Contractor, terms as defined in the applicable Privacy Laws.

4. **DATA PRIVACY**

Licensee hereby certifies that it will:

4.1 Comply with Privacy Laws and use all reasonable endeavors to assist OATS in its own compliance with Privacy Laws in connection with this DPA. This includes that Licensee will (i) provide notice to, and obtain consent from, Data Subjects as appropriate and in accordance with Privacy Laws, and (ii) assist with privacy impact assessments;

4.2 Immediately inform OATS in writing if the Licensee cannot meet its obligations under this DPA. Details regarding the Processing are in Exhibit B attached to this DPA as required by Privacy Laws;

4.3 Not do, cause, or permit to be done anything in relation to the information provided to or processed by Licensee that may result in a breach by OATS of any applicable laws, regulations, regulatory requirements, or Privacy Laws;

4.4 Not use, engage, or practice any Dark Patterns in performing Work, incorporate any Dark Patterns in Work Product provided to OATS, or permit its subcontractors or subprocessors to do so.

4.5 Only process the Personal Data in accordance with OATS's documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of Licensee's obligations under this DPA, unless otherwise required by law. In particular, Licensee shall not: (i) sell the Personal Data or share the Personal Data with any third parties without OATS's permission; (ii) retain, use, or disclose the Personal Data for any purpose other than the purposes specified in the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than to use the Licensed IP to offer technology training to seniors as contemplated in the Agreement; (iii) retain, use, or disclose the Personal Data outside of Licensee's direct business relationship with OATS; and (iv) combine the Personal Data with information received from or on behalf of another person or entity, or the Personal Data that Licensee collects from its own interactions with Data Subjects;

4.6 Put in place measures to ensure that access to the Personal Data is limited to employees who have a need to access the Personal Data for the purposes specified in this DPA and/or elsewhere in the Agreement. Any employees who have access to the Personal Data: (i) must not process the data except on instructions from OATS, unless required to do so by law; (ii) must be subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and (iii) must comply with applicable Privacy Laws in the context of that individual's duties to OATS;

4.7 Not disclose the Personal Data to any other person or entity, including any subprocessor or Generative AI Platform, without OATS's express agreement in writing;

4.8 Not subcontract to a subprocessor any of Licensee's duties under this DPA unless: (i) Licensee has obtained prior express agreement in writing from OATS; (ii) the subprocessor is subject to a written agreement that imposes on the subprocessor the same obligations that are imposed on Licensee under this DPA, and (iii) Licensee has carefully chosen the subprocessor under consideration of the appropriateness of the technical and organizational security measures taken by the subprocessor. OATS may object to the engagement of a new subprocessor. If OATS objects, the Parties shall work together in good faith to agree on a reasonable solution, which may include termination of this DPA without penalty. Any consent that OATS gives pursuant to this clause or this DPA generally for subcontracting will not relieve Licensee from any liability for the performance of its obligations under this DPA;

4.9 Only store and process the Personal Data within the United States;

4.10 Comply with all reasonable requests or directions by OATS to enable it to verify and/or procure that Licensee is in full compliance with its obligations under this DPA; and

4.11 Upon termination of the Agreement, delete or return all Personal Data to OATS, at its discretion, and delete any existing copies of the Personal Data, save where applicable law requires Licensee to retain copies of such data. Licensee shall provide written certification to OATS that it and each of its subprocessors have fully complied with this section within sixty (60) calendar days of the termination of the Agreement. Where Licensee is required to maintain Personal Data to meet legal obligations, Licensee must delete Personal Data within sixty (60) days of the termination of that requirement and provide OATS with written certification that it and each of its subprocessor have fully complied with this section.

5. **DATA SUBJECT REQUESTS**

5.1 If OATS provides written notification to Licensee of a Data Subject's request to exercise rights related to Personal Data under Privacy Laws, Licensee shall assist OATS insofar as reasonably possible in responding.

5.2 If Licensee receives a complaint or request relating to Privacy Laws, Licensee shall promptly notify OATS.

6. **SECURITY.**

Licensee hereby certifies as following:

6.1 **Security Controls.** Licensee shall maintain a written information security program with respect to Confidential Information and Personal Data that contains appropriate administrative, technical, and physical safeguards designed, at a minimum, to: (i) ensure the security and confidentiality of Confidential Information and/or Personal Data; (ii) protect against reasonably anticipated threats or hazards to the security or integrity of Confidential Information and/or Personal Data; and (iii) protect against unauthorized access to or use of Confidential Information and/or Personal Data. All of the foregoing shall be consistent with and be no less rigorous than those safeguards and procedures required by applicable laws and regulations, including, without limitation, all applicable Privacy Laws. Licensee shall protect and maintain the security and confidentiality of the Confidential Information and/or Personal Data using at least the same level of care (but no less than reasonable care) that Licensee uses to protect and maintain the

security and confidentiality of its own confidential information and/or Personal Data, as applicable. To the extent that Licensee has access to Personal Data and/or Confidential Information that OATS deems to be particularly sensitive, Licensee shall, at a minimum, adhere to an industry accepted security standard such as ISO 27001 standards, the NIST Cybersecurity Framework, or such other standards upon which the Parties may mutually agree to ensure the security and protection of Personal Data, taking into account the nature and sensitivity of the information to be protected, the risk presented by Processing, the state of the art, and the costs of implementation, in compliance with applicable Privacy Laws. If Licensee Processes, transmits, or stores OATS payment card data, Licensee shall also adhere to and comply with the current Payment Card Industry Data Security Standards ("PCI DSS"). In the event that OATS is unable to confirm to its reasonable satisfaction Licensee's compliance with such requirements, then OATS shall be entitled, upon notice to Licensee, to terminate the Agreement with Licensee without penalty.

6.2 **Incidents**

6.2.1 **Notice of Incidents.** Licensee shall maintain a written data compromise incident response plan that contains, at a minimum, the following: (i) roles, responsibilities, and communication strategies in the event of a compromise, and (ii) specific incident response procedures. Licensee shall notify OATS as soon as practicable, but no later than forty-eight (48) hours following discovery, if Confidential Information and/or Personal Data was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. Licensee agrees to make available sufficient resources and data for OATS to determine the full impact and root cause of the incident, and to cooperate with OATS in the execution of OATS's security incident response plans, including, at OATS's request, cooperation with any law enforcement or regulatory officials, credit reporting companies, credit card associations, or others investigating such incident.

6.2.2 **Data Breach.** Licensee shall immediately notify OATS if Licensee knows, discovers, or reasonably **believes** that there has been any Data Breach. In the event of a Data Breach, Licensee shall (i) immediately investigate, correct, mitigate, remediate, and otherwise handle the Data Breach, including without limitation, by identifying Personal Data affected by the Data Breach and taking sufficient steps to prevent the continuation and recurrence of the Data Breach; and (ii) provide information and assistance needed to enable OATS to evaluate the Data Breach and, as applicable, to comply with any obligations to provide timely notice to affected individuals or information about the Data Breach to relevant regulators; and

6.2.3 Licensee shall reimburse OATS for the reasonable expenses that OATS may incur as a result of such Data Breach caused by Licensee's acts or omissions or those of any of Licensee's authorized subprocessors, including but not limited to the expenses incurred in investigating the Data Breach, notifying affected individuals, and providing these individuals with the support necessary under the circumstances, such as credit monitoring.

6.3 **Assessments**

Licensee will maintain accurate and detailed records of its performance of its obligations under this Agreement.

6.3.1 OATS reserves the right to perform, either itself or through an authorized representative, security posture assessments relating to Licensee's use of the Licensed IP and obligations under this Agreement ("Assessments"). Assessments may include on-site or remote examinations of Licensee's and/or its subprocessors' internal controls (such as business, security, and information technology practices) relevant to this Agreement. Without limiting Licensee's obligations with respect to Confidential Information or Personal Data, OATS shall have the right to have its designated representative or representatives at Licensee's and/or its subprocessors' premises, to observe and monitor the performance of the Work, and ensure that adequate security controls are in place. OATS agrees that any access to Licensee's and/or its subprocessors' premises will be at a mutually convenient time and in a manner that minimizes interference with business operations. Licensee will make all directly pertinent records available for inspection or assessment by OATS or its authorized agent at Licensee's business office during normal business hours for the term of this Agreement and for two (2) years after the termination of this Agreement and each SOW. Unless OATS reasonably believes that a breach of confidentiality or Data Breach may have occurred, OATS shall not conduct more than one (1) Assessment per calendar year and will provide at least fifteen (15) calendar days' advance notice of Assessment. In addition to the foregoing, the Licensee shall share results of any external audit report (e.g., SOC2, Type II or PCI) completed within the last twelve (12) months to verify its compliance with standards outlined in Section 6.1 above. The scope of such audit report must include all OATS relevant systems to be considered, at OATS's discretion, an alternative to OATS conducting its own on-site Assessment.

6.3.2 Licensee agrees to remediate any issues identified as a result of an Assessment within ninety (90) calendar days unless otherwise mutually agreed upon between Licensee and OATS. In the event that the Parties are unable to agree, either Party will have the right to terminate the Agreement upon written notice to the other Party without penalty.

7. CERTIFICATION AND VIOLATION RIGHTS

7.1 OATS reserves the right in its sole discretion to determine the appropriate action to be taken in the event that Licensee violates this DPA. Such action may include OATS's termination of the existing Agreement.

7.2 Licensee certifies that Licensee understands the restrictions herein and will comply with them.

8. LIABILITY

Notwithstanding anything to the contrary elsewhere in the Agreement, any limitations on Licensee's total aggregate liability, including any liability for subprocessors, shall exclude breaches under or in connection with this DPA.

9. INSURANCE

Licensee presently maintains and will continue to maintain in force, at Licensee's sole expense, the following insurance: Cyber Risk and Privacy Liability Insurance Policy, or similar policy with a nationally recognized insurance company and OATS as a named insured having a minimum limitation of liability of Two Million US Dollars ($2,000,000). If the Licensee is a government or public

agency, it may self-insure the terms of coverage or contract with an insurance company to provide substantially equivalent coverage.

10. **INDEMNITY**
    Notwithstanding anything else in the Agreement, hereunder, or otherwise, Licensee's indemnification obligations shall include all third-party claims and legal actions brought against OATS arising out of Licensee's breach or alleged breach of this DPA and shall be excluded from any indemnification limitations; provided, however, that if Licensee is a government or public entity with restrictions on indemnification, indemnification shall be to the full extent permissible by law.

Exhibit A

1. DEFINITIONS

1.1 "Biometric information" means a person's physiological, biological, or behavioral characteristics, including DNA-related information, that could be used by itself or in combination with other data to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

1.2 "Collection" means gathering or obtaining Personal Data from any source and in any manner (including verbally or in written or electronic format), including directly from the Data Subject or from a third party, such as a Data Broker.

1.3 "Contract Documents" means any executed contract(s) that reference this DPA and are currently in effect between OATS and Licensee.

1.4 "Dark Pattern" means a user interface designed to influence the choice of the user, with the substantial effect of manipulating, subverting, or impairing user autonomy, decision-making, or choice, or as defined by Privacy Laws.

1.5 "Data Broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom such business does not have a direct relationship.

1.6 "Data Subject" means a living human person who is the subject of any of the Personal Data.

1.7 "Data Breach" means any accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, acquisition of, or use of any Personal Data.

1.8 "Personal Data," or "Personal Information," shall mean (a) any information that Licensee has received or collected for Processing pursuant to the Agreement that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular Data Subject or household, or (b) any information that is defined as "personal data" or "Personal Data" by applicable Privacy Laws. Personal Data includes all logs and any other materials, such as metadata, inferences made by analyzing other Personal Data, Probabilistic Identifiers, and pseudonyms used as Data Subject identifiers, collected or generated by OATS to the extent such materials contain Personal Data. "Personal Data" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this definition, "publicly available" means information that is lawfully made available from federal, state, or local government records, or information that OATS has a reasonable basis to believe is lawfully made available to the general public by the Data Subject or from widely distributed media or is defined by an applicable state statute. "Publicly available" does not mean biometric information collected by a business about a Data Subject without the Data Subject's knowledge.

1.9 “Precise Geolocation Data,” or “Geolocation Data,” means any data that is derived from a device and that is used or intended to be used to locate a Data Subject within a geographic area of a radius of 1,750 feet or less, or as defined by applicable Privacy Laws.

1.10 “Privacy Laws” means all laws, guidelines, and regulations, in any country or jurisdiction that protect the privacy rights of individuals, insofar as those laws and regulations apply to the Processing of Personal Data, including, without limitation, the California Privacy Rights Act; the Virginia Consumer Data Protection Act; the Utah Consumer Privacy Act; the Connecticut Act Concerning Personal Data Privacy and Online Monitoring; and the Colorado Privacy Act; and any other laws that may take effect impacting the Processing of Personal Data.

1.11 “Probabilistic Identifier” means the certainty of identification of a Data Subject (or their device) to a degree more probable than not, based on any categories of Personal Data in the definition of Personal Data.

1.12 “Processing” and “Process” shall mean any activities or operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.13 “Profiling” means any form of automated processing of Personal Data, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning such person’s purchases, performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements or as defined by applicable Privacy Laws.

1.14 “Sell,” “selling,” “sale,” or “sold,’’ means selling, renting, releasing, disclosing, disseminating, making available, transferring, sharing, exchanging, or otherwise communicating orally, in writing, or by electronic or other means Personal Data by a business to a third party for monetary or other valuable consideration. Personal Data is not sold when:

(i) A Data Subject uses or directs the business to intentionally disclose Personal Data;
(ii) The business uses or shares an identifier for a Data Subject who has opted out of the sale of the Data Subject’s Personal Data or limited the use of the Data Subject’s sensitive Personal Data for the purposes of alerting persons that the Data Subject has opted out of the sale of the Data Subject’s Personal Data or limited the use of the Data Subject’s sensitive Personal Data; or
(iii) The business transfers to a third party the Personal Data of a Data Subject as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared in a manner that is the same or substantially similar.

1.15 “Sensitive Personal Data” means Personal Data that reveals the following about a Data Subject:

(i) Social Security, driver’s license, state identification card, or passport number;

(ii) Account login or financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
(iii) Precise geolocation;
(iv) Racial or ethnic origin, religious or philosophical beliefs, or union membership;
(v) Contents of mail, email, and text messages, unless the business is the intended recipient of the communication;
(vi) Genetic data;
(vii) Biometric information;
(viii) Health information; or
(ix) Sex life or sexual orientation.

1.16 "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, exchanging, or otherwise communicating orally, in writing, or by electronic or other means Personal Data by the business to a third party.

For the purposes of this definition, Sharing does not include instances where:

(i) A Data Subject uses or directs the business to intentionally disclose Personal Data or intentionally interact with one or more third parties;
(ii) The business uses or shares an identifier for a Data Subject who has opted out of the sharing of the Data Subject's Personal Data or limited the use of the Data Subject's sensitive Personal Data for the purposes of alerting persons that the Data Subject has opted out of the sharing of the Data Subject's Personal Data or limited the use of the Data Subject's sensitive Personal Data; or
(iii) The business transfers to a third party the Personal Data of a Data Subject as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared in a manner that is the same or substantially similar.

EXHIBIT B

DETAILS OF PROCESSING

This Exhibit is required by various US Privacy Laws. No exchange, transfer, processing, transmission, or any other use of Personal Data between the Parties is permitted unless recorded below. Refer to "Definitions" set forth in Exhibit A as needed.

Required Detail	Response	Notes/Details
A. Categories of Data Subjects whose Personal Data is transferred and processed under this DPA (check the applicable categories)	☒ Employees including temporary workers, contractors and job applicants ☒ Consumers ☒ Website and digital asset users ☐ Suppliers and other business contacts	
B. Categories of Personal Data transferred and processed under this DPA (electronic or physical form) (check the applicable categories)	☒ 1. Personal Identifiers	Such as a name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, driver's license number, passport number, Probabilistic Identifier, or other similar identifiers as permitted by OATS
	☒ 2. Customer Records	Such as name, signature, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, or Probabilistic Identifier
	☒ 3. Commercial Information: Goods or services provided and related information	Including details of the goods or services supplied, records of personal property, licenses issued, contracts, or purchasing or consuming histories
	☒ 4. Characteristics of protected classifications under law	Such as race, ancestry, national origin, religion, age, mental or physical disability, sex, sexual orientation, gender identity, medical condition, genetic information, marital status, or military status – but only so far as permitted by OATS in this DPA
	☒ 5. Internet or other electronic network activity information	Such as browsing history, search history, or information regarding a Data Subject's interaction with a website, application, or advertisement

Required Detail	Response	Notes/Details
	☐ 6. Audio, electronic, visual, thermal, olfactory, or similar information	
	☒ 7. Professional or employment-related information	Including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, or security records
	☒ 8. Education information not considered publicly available	Education and training details, including information that relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil record, or as otherwise defined in the Family Educational Rights and Privacy Act
	☒ 9. Inferences that can create a profile about a Data Subject	Reflects the Data Subject's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes
	☒ 10. Family, lifestyle, and social circumstances	Including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organizations.
	☒ 11. Financial details	Including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.
	☐ 12. Personal Data relating to criminal convictions and offences.	
	☒ 13. Sensitive Personal Information	

Required Detail	Response	Notes/Details
	☐ a. Social Security, driver's license, state identification card, or passport number ☐ b. account login or financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account ☐ c. precise geolocation ☒ d. racial or ethnic origin, religious or philosophical beliefs, or union membership ☐ e. contents of mail, email, and text messages, unless the business is the intended recipient of the communication ☐ f. genetic data ☐ g. biometric information ☒ h. health information ☐ i. sex life or sexual orientation	
	☐ 14. Other (provide details):	
C. The frequency of the transfer and processed under this DPA (check the applicable response)	☐ Data transferred on one-off basis ☒ Data transferred and processed under this DPA on continuous basis.	
D. Nature of Processing of Data	☒1. Collecting	Includes buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a Data Subject by any means approved by OATS in writing, including by observing the consumer's behavior through technological means.
	☒ 2. Receiving	Includes collection, accessing, retrieval, recording, and data entry
	☒ 3. Holding	Includes storage, organization, and structuring
	☒ 4. Using	Includes analyzing, consultation, testing, automated decision making, and profiling
	☒ 5. Updating	Includes correcting, adaptation, alteration, alignment, and combination
	☒ 6. Protecting	Includes restricting, encrypting, and security testing

Required Detail	Response	Notes/Details
	☒ 7. Sharing	Includes disclosure, dissemination, allowing access, or otherwise making available
	☒ 8. Returning data to OATS or data subject	
	☒ 9. Erasing	Includes destruction and deletion
	☒ 10. Other (provide details):	
E. Purpose(s) of the data transfer and further Processing	As described in the Agreement	
F. Retention Period, or if not possible, criteria used to determine Retention Period	For as long as required for the purposes indicated above and for the period set forth in the Agreement and applicable SOWs and in accordance with general data protection guidelines regarding record retention policies	At OATS's direction, Licensee will delete or return all Personal Data to OATS at any time as requested and at the end of the Agreement, unless retention of the Personal Data is required by law
G. Subject-matter of the Processing	As defined in the DPA and elsewhere in the Agreement	
H. Duration of the Processing	For the term designated under the Agreement or any SOW as applicable	