

SENECTA DATA PROCESSING ADDENDUM

Last updated: 26 August 2026

This Data Processing Addendum ("DPA") forms part of the monitoring service agreement (the "Agreement") between **Senecta, Inc. ("Senecta")** and the customer that has entered into it ("**Customer**"). Capitalised terms not defined here have the meaning given in the Agreement.

Where a customer has executed a negotiated DPA as an exhibit to its Agreement, that document governs and this one does not apply.

1. Definitions

1.1 "**Applicable Privacy Law**" means all US federal and state laws relating to the processing of personal information that apply to a Party's performance, including the California Consumer Privacy Act as amended by the CPRA ("**CCPA**"), the Washington My Health My Data Act, the Nevada consumer health data law (SB 370), and the comprehensive consumer privacy statutes of other states as they take effect.

1.2 "**Personal Information**" means information within Resident Data or Customer Data that identifies, relates to, describes, or is reasonably capable of being associated with an identified or identifiable natural person, and includes Consumer Health Data.

1.3 "**Consumer Health Data**" means Personal Information that identifies a Consumer's past, present, or future physical or mental health status, as defined under the Washington My Health My Data Act and equivalent state laws.

1.4 "**Consumer**" or "**Data Subject**" means the natural person to whom Personal Information relates, including Residents, other members of a Household, persons attending a Residence, and Authorized Users.

1.5 "**Business Purpose**" means the provision, operation, security, support, and improvement of the Service in accordance with the Agreement, and no other purpose.

1.6 "**Security Incident**" means a breach of Senecta's security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to Personal Information. It does not include unsuccessful attempts or activity that does not compromise security, such as pings, port scans, or failed log-in attempts.

1.7 "**Subprocessor**" means a third party engaged by Senecta to process Personal Information on Senecta's behalf.

1.8 The terms **Business**, **Service Provider**, **Sell**, **Share**, **Cross-Context Behavioral Advertising**, **Controller**, **Processor**, and **Deidentified** have the meanings given in Applicable Privacy Law.

2. Roles of the Parties

2.1 For Resident Data, Customer is the Business and Controller and Senecta is the Service Provider and Processor. Customer determines the purposes and means of processing.

2.2 For account details, billing records, and Authorized User contact information, Senecta acts as a Business and Controller in its own right, for contracting, billing, account administration, security, and its own legal compliance. That processing is described in Senecta's Privacy Policy.

2.3 Each Party is independently responsible for its own compliance with Applicable Privacy Law in respect of the roles it holds.

2.4 Customer is responsible for obtaining all consents and giving all notices required in connection with the installation and operation of the Sensors, including under state wiretapping, eavesdropping, and all-party consent laws, and for the lawfulness of its instructions to Senecta.

3. Scope and purpose limitation

3.1 Senecta will process Personal Information only on Customer's documented instructions, which comprise the Agreement, this DPA, and Customer's use of the Service, and only for the Business Purpose.

3.2 Senecta will not:

- (a) Sell or Share Personal Information;
- (b) use or disclose Personal Information for Cross-Context Behavioral Advertising or targeted advertising;
- (c) retain, use, or disclose Personal Information for any purpose other than the Business Purpose, including any commercial purpose of its own, except as expressly permitted by Section 6;
- (d) retain, use, or disclose Personal Information outside the direct business relationship between the Parties; or
- (e) combine Personal Information received under the Agreement with personal information obtained from any other source, except as permitted for a Service Provider under the CCPA.

3.3 Senecta certifies that it understands and will comply with the restrictions in Section 3.2.

3.4 Senecta will notify Customer promptly if it determines that it can no longer meet its obligations under Applicable Privacy Law. Customer may then direct Senecta to stop the processing concerned or to take reasonable steps to remediate.

3.5 Senecta will not process Personal Information in a manner inconsistent with any executed Business Associate Agreement. Where data constitutes protected health information, that agreement prevails over this DPA.

4. Confidentiality and personnel

4.1 Senecta limits access to Personal Information to personnel who need it to deliver the Service.

4.2 Those personnel are bound by written confidentiality obligations and receive training appropriate to their role, including on the handling of Consumer Health Data.

5. Security

5.1 Senecta will implement and maintain reasonable administrative, physical, and technical security measures, appropriate to the nature of the Personal Information and to the risks presented by its processing, including its Consumer Health Data elements. Those measures include encryption in transit and at rest, role-based access control, and logging of access to Resident Data.

5.2 Senecta will not materially reduce the overall level of security protection during the term.

5.3 Senecta will provide reasonable assistance with any data protection or risk assessment Customer is required to carry out in relation to the Service.

6. Sensing and audio processing

6.1 Senecta Sensors combine radar (radio frequency) sensing and acoustic sensing. The Sensors contain no camera and capture no images or video. Radar detects movement, presence, and position within a room and produces no visual representation of any person.

6.2 Ambient audio captured by the Sensors is analysed automatically by Senecta's algorithms in order to generate Insights. Raw audio is not made available to Senecta personnel, to Customer, or to any third party, and no person listens to it. Only the derived Insights are exposed through the Service.

7. Deidentified data

7.1 Senecta may create Deidentified data from Personal Information and use it to operate, secure, and improve the Service, to develop, train, and improve the models underlying the Service, and to develop new products. Senecta may retain and use that data indefinitely, including after termination.

7.2 Senecta will take reasonable measures to ensure Deidentified data cannot be associated with a Consumer or Household, will maintain it in deidentified form, will not attempt to reidentify it, and will bind any recipient to the same restrictions.

7.3 Senecta will not use Deidentified data to contact, profile, or make any decision about an individual Consumer.

8. Subprocessors

8.1 Customer authorises Senecta to engage Subprocessors for the following categories of service: cloud hosting, storage and compute; payment processing; email and application messaging; error monitoring and application telemetry; and product and website analytics. A current list identifying each Subprocessor by name, purpose, and location is available on written request.

8.2 Senecta will give Customer at least thirty (30) days' written notice before engaging a new Subprocessor. Customer may object on reasonable data protection grounds within fifteen (15) days. The Parties will work in good faith to resolve the objection, and if they cannot, Customer may cancel the subscription without penalty. That is Customer's sole remedy.

8.3 Senecta imposes on each Subprocessor written obligations no less protective than those in this DPA, and remains responsible to Customer for each Subprocessor's performance.

8.4 All Subprocessors process and store Personal Information within the United States. Senecta will not transfer Personal Information outside the United States without Customer's prior written consent.

9. Consumer rights

9.1 Senecta will provide reasonable assistance to enable Customer to respond to a Consumer's request to access, correct, delete, port, limit the use of, or opt out of the processing of their Personal Information.

9.2 If Senecta receives such a request directly, it will not respond substantively and will forward the request to Customer without undue delay, unless Applicable Privacy Law requires otherwise.

9.3 Where Customer instructs Senecta to delete, correct, or restrict Personal Information to honour a Consumer request, Senecta will do so within thirty (30) days and will pass the instruction to its Subprocessors.

10. Security incidents

10.1 Senecta will notify Customer of a Security Incident without undue delay and in any event within seventy-two (72) hours of becoming aware of it.

10.2 The notification will describe, to the extent known, the nature of the incident, the categories and approximate number of Consumers and records affected, the likely consequences, and the measures taken or proposed.

10.3 Senecta will investigate, take reasonable steps to mitigate and remediate, and provide the information Customer reasonably requires to meet its own notification obligations. Senecta will not publicly identify Customer in connection with a Security Incident without Customer's prior written consent, unless legally required.

10.4 Notification is not an acknowledgement of fault or liability.

11. Audit and assurance

11.1 On written request, and no more than once in any twelve (12) month period, Senecta will complete Customer's standard security questionnaire and provide a written description of its then-current security measures. The Parties agree this ordinarily satisfies Customer's audit rights. Senecta does not currently hold a SOC 2 or ISO 27001 certification, and will provide the report or certificate in place of the questionnaire once one is obtained.

11.2 Where Applicable Privacy Law requires a further audit, Customer may, on thirty (30) days' written notice, conduct or appoint an independent auditor to conduct an audit of Senecta's processing, during business hours, subject to confidentiality obligations, at Customer's expense, and in a manner that does not unreasonably disrupt Senecta's operations.

12. Retention, return and deletion

12.1 Senecta retains Personal Information only for as long as necessary for the Business Purpose. For an active Household, that includes retaining its history for the duration of activation so that longitudinal Insights can be generated.

12.2 Customer may export Personal Information relating to its clients in a machine-readable format at any time during the term and for thirty (30) days after termination.

12.3 Senecta will delete or return all Personal Information within thirty (30) days after termination, except to the extent retention is required by law. Where retention is required, Senecta will continue to protect the data under this DPA and will delete it when the obligation ends.

12.4 Deletion from backup media occurs on Senecta's ordinary backup cycle, not exceeding thirty-five (35) days, during which the data remains protected under this DPA and is not actively processed.

13. General

13.1 In the event of conflict, any executed Business Associate Agreement prevails as to protected health information, then this DPA, then the body of the Agreement.

13.2 Each Party's liability under this DPA is subject to the limitation of liability provisions of the Agreement.

13.3 This DPA takes effect on the effective date of the Agreement and continues for as long as Senecta processes Personal Information under it.

13.4 If a change in Applicable Privacy Law requires amendment, the Parties will negotiate the amendment in good faith and without unreasonable delay.

ANNEX: DETAILS OF PROCESSING

Subject matter. Provision of the Senecta ambient monitoring Service to Customer.

Duration. The term of the Agreement, plus the retention periods in Section 12.

Nature and purpose. Collection of ambient sensor data in Households; processing of that data to detect events and generate Insights; delivery of alerts, dashboards, and reports to Authorized Users; support, security, and service improvement.

Categories of Data Subject

- Residents
- Other members of a Household and visitors present in a Residence
- Caregivers and other workers attending a Residence
- Authorized Users of Customer

Categories of Personal Information

- Radar sensing data indicating movement, presence, and position, containing no images or video
- Ambient audio, processed automatically as described in Section 6
- Derived Insights, including movement pattern changes, cough frequency trends, vocalization and conversation activity levels, and bathroom-visit frequency
- Residence address and Resident identifier supplied by Customer
- Authorized User account details and access logs

Sensitive Personal Information / Consumer Health Data. The Insights listed above constitute Consumer Health Data under the Washington My Health My Data Act and equivalent state laws, and are treated as Sensitive Personal Information under the CCPA.

Frequency of processing. Continuous for the duration of each Household's activation.

Location of processing. United States. Production infrastructure is located in Hillsboro, Oregon.