Data Processing Agreement

Version: 2.3

Document Revision History:

AUTHOR	REVISION	COMMENTS	DATE
Dor Daniel	1.0	First draft	10/4/2025
Roy Coren	2.0	SOC2 /HIPAA Alignment	14/01/26
Roy Coren	2.1	Technical stack	06/04/26
Dor Daniel	2.2	Added customer deletion request	17/05/26
Roy Coren	2.3	Consolidated with legal reviews	28/05/26

Table of content

1. Introduction..... 2
2. DEFINITIONS AND INTERPRETATION..... 3
3. PROCESSING OF COMPANY PERSONAL DATA..... 4
4. PROCESSOR PERSONNEL (SOC 2 CC1.0 - CC5.0)..... 5
5. SECURITY OF PROCESSING (SOC 2 CC6.0 - CC7.0)..... 5
6. SUBPROCESSING & VENDOR RISK MANAGEMENT..... 6
7. DATA SUBJECT RIGHTS & ASSISTANCE..... 7
8. PERSONAL DATA BREACH (SOC 2 CC7.3)..... 7
9. AUDIT RIGHTS & SOC 2 COMPLIANCE..... 8
10. DATA PROTECTION IMPACT ASSESSMENT (DPIA)..... 9
11. DELETION OR RETURN OF DATA..... 9
12. DATA TRANSFERS..... 10
13. GENERAL TERMS..... 10
14. SCHEDULE 1: DETAILS OF PROCESSING..... 11
15. SCHEDULE 2: TECHNICAL & ORGANIZATIONAL MEASURES (TOMs)..... 11

1. Introduction

This Data Processing Agreement ("Agreement") forms part of the Contract for Services under Longevity AI's Terms and Conditions (the "Principal Agreement") between Longevity AI LTD, VAT No. 516459625, Amir Gilboa 7, Apt 18, Tel Aviv 6967136, Israel (referred to as "Longevity AI" or "Processor") and the Company using Longevity AI's services (referred to as the "Company" or "Controller"). Company and Processor shall be collectively referred to as the "Parties", and each a "Party".

By entering into the Principal Agreement, the Company expressly accepts and agrees to be bound by this Agreement, which forms an integral part of, and constitutes an addendum to, the Principal Agreement. This Agreement shall apply to the extent that the Processor processes Company Personal Data on behalf of the Company to provide the Services, and its provisions shall prevail in relation to such processing activities.

WHEREAS:

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services which imply the processing of Personal Data and Protected Health Information (PHI).

(C) The Parties seek to implement a DPA that complies with GDPR, HIPAA, and the AICPA Trust Services Criteria (SOC 2).

(D) The Processor operates a multi-tenant SaaS environment hosted on Amazon Web Services (AWS).

2. DEFINITIONS AND INTERPRETATION

2.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

- "Agreement" means this Data Processing Agreement and all Schedules and Exhibits attached hereto.
- "Applicable Laws" means any applicable law, including Data Protection

Laws, to which the Processor is subject with respect to any Personal Data.

- "Company Personal Data" means any Personal Data or Protected Health Information (PHI) related to the Company's customers, patients, or employees, which is Processed by the Processor or any Sub-processor on behalf of the Company as part of the performance of the Services under the Principal Agreement.
- "Data Protection Laws" means, as applicable, (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR") and any member state implementations; (ii) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA", 45 C.F.R. Parts 160-164); (iii) the Israeli Privacy Protection Law, 5741-1981; and (iv) all applicable data protection or privacy laws, rules, and regulations of any other country, as amended, adopted, or superseded from time to time.
- "Security Standards" means the AICPA Trust Services Criteria for Security, Availability, and Confidentiality (SOC 2).
- "Services" means the personalized, AI-driven digital health services designed to support medical professionals in predicting and managing chronic diseases provided under the Principal Agreement.
- "Sub-processor" means any third party appointed by or on behalf of the Processor (excluding any personnel member of the Processor) to process Company Personal Data on behalf of the Company and for its benefit in connection with the Services.

2.2. The terms "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the meaning ascribed to them (or their equivalents) in the applicable Data Protection Laws.

3. PROCESSING OF COMPANY PERSONAL DATA

3.1. Instructions: For the purposes of this Agreement, the Company may act as either a data controller or a data processor, as applicable, and the Processor may act as either a data processor or a sub-processor,

depending on the nature of the processing activities and the instructions of the Company.

3.2. The Processor shall not process Company Personal Data other than on Controller's documented instructions, where such instructions are consistent with the terms of the Principal Agreement, unless otherwise required by Applicable Law, in which case Processor shall, to the extent permitted by Applicable Law, inform the Company of such legally required Processing of Company Personal Data, unless that law prohibits such information on important grounds of public interest.

3.3. Scope of Authorization: The Company hereby instructs the Processor to process Company Personal Data to: (a) provide the Services, including related technical support; (b) fulfill its legal obligations or resolve disputes; and (c) exercise any internal task aimed to optimize the security, privacy, confidentiality, and functionalities of the Services. Additional instructions outside this scope require prior written agreement and may include additional fees.

3.4. HIPAA Compliance: To the extent the Processor processes PHI, the Processor shall comply with the Business Associate Agreement (BAA) standards as required by 45 C.F.R. § 164.314.

3.5. Anonymized Data: The Company acknowledges and agrees that the Processor may collect, disclose, publish, share, and use fully anonymized, de-identified, and aggregated data derived from Company Personal Data for legitimate purposes, including maintaining, operating, and improving the Services and for research purposes. The Processor agrees not to use said anonymized data in a form that identifies the Company or any Data Subject. Company hereby agrees and acknowledges that such processing activities (including the anonymization and de-identification of Personal Data) will not be considered as

performed outside the scope of the Instructions provided by Company hereunder.

3.6. Data Legitimacy: The Company shall have sole responsibility for the accuracy, quality, and legality of the Company Personal Data and the means by which it was acquired. The Company warrants that the data has been collected and transferred in accordance with applicable laws, including obtaining required consents from Data Subjects regarding international transfers.

4. PROCESSOR PERSONNEL (SOC 2 CC1.0 - CC5.0)

4.1. Reliability and Authorization: The Processor will be responsible for using qualified personnel with data protection training to provide the Services and ensure that access to Company Personal Data is limited only to those personnel who require such access on a strict "need-to-know" basis.

4.2. Background Checks: In accordance with SOC 2 requirements, all Processor personnel with access to the production environment undergo background checks (to the extent permitted by local law).

4.3. Confidentiality Obligations: The Processor shall obligate its personnel to Process Company Personal Data only in accordance with this Agreement. The Processor ensures that its personnel have committed themselves to binding confidentiality undertakings or are under an appropriate statutory obligation of confidentiality.

5. SECURITY OF PROCESSING (SOC 2 CC6.0 - CC7.0)

5.1. Technical Measures: Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of

Processing, the Processor has implemented and will maintain the Technical and Organizational Measures (TOMs) specified in Schedule 2 to ensure a level of security appropriate to the risks.

5.2. Encryption Standards: The Processor shall ensure Company Personal Data is encrypted: (i) At Rest using AES-256 or stronger via AWS KMS; and (ii) In Transit using TLS 1.2 or higher across all public and internal endpoints.

5.3. Logical Separation: As a multi-tenant SaaS provider, the Processor shall maintain strict logical isolation and multi-tenant separation of Company Personal Data via unique tenant identifiers to prevent cross-customer data access.

5.4. Infrastructure Management: The Services are hosted on Amazon Web Services (AWS). The Processor is responsible for managing the logical security of the application, while AWS manages physical and environmental security.

6. SUBPROCESSING & VENDOR RISK MANAGEMENT

6.1. General Authorization: The Company hereby grants general authorization to the Processor to engage Sub-processors as necessary to provide the Services. The authorized Sub-processors are listed in the Processor's operational infrastructure records e.g., AWS, Firebase(google), Stripe, Spike).

6.2. Notification of Changes and Objection Rights: The Processor shall regularly maintain and update its list of Sub-processors. The Processor will inform the Company of any intended changes or updates to the Sub-processors list. The Company may reasonably object to such changes under legitimate and documented grounds within fourteen (14) days of notification. If an objection is legitimate, the Processor shall either refrain from using the Sub-processor or notify the Company that it is unable to

provide the Services without them, thereby allowing immediate suspension or restriction of the affected Services.

6.3. Flow-Down & Liability: The Processor shall ensure that Sub-processors are bound by written terms no less restrictive and protective than this Agreement. Where the Sub-processor fails to fulfill its obligations, the Processor shall remain fully liable to the Company for the performance of that Sub-processor's obligations.

6.4. SOC 2 Vendor Oversight: The Processor shall perform annual risk assessments of its material Sub-processors (including reviewing their SOC 2 Type II or ISO 27001 reports) to ensure the continued security of the supply chain.

7. DATA SUBJECT RIGHTS & ASSISTANCE

7.1. Assistance: Taking into account the nature of the processing, the Processor shall provide reasonable assistance (including technical tools within the SaaS platform) to enable the Controller to respond to Data Subject requests (e.g., access, erasure, correction).

7.2. Notification: The Processor shall promptly, and in any event within five (5) business days, notify the Company if it receives a request directly from a Data Subject. The Processor shall not respond directly to that request except on the documented instructions of the Controller or as required by Applicable Laws.

8. PERSONAL DATA BREACH (SOC 2 CC7.3)

8.1. Notification: In the event of a Personal Data Breach affecting Company Personal Data, the Processor shall notify the Company without undue delay, and where feasible, within seventy-two (72) hours of becoming aware of the breach, providing sufficient information to enable the Company to fulfill its obligations under Data Protection Laws.

8.2. Report Contents: The notification shall include the nature of the breach, the categories of data and data subjects affected, the likely consequences, and the Processor's immediate mitigation and remediation plan. If full information is unavailable initially, the Processor shall provide a phased supplement as it becomes available.

8.3. Remediation & Cooperation: The Processor shall take reasonable commercial steps to mitigate the effects and prevent recurrence, and shall reasonably cooperate with the Company in the investigation and remediation of each such breach.

9. AUDIT RIGHTS & COMPLIANCE (SOC 2 CC4.0)

9.1. Evidence of Compliance: Processor shall make available all information necessary to demonstrate compliance. This shall be satisfied by providing the Company with its most recent SOC 2 Type II Report (or, prior to the first audit, a Letter of Engagement from an accredited CPA firm).

9.2. On-Site Inspection: If the provided SOC 2 report does not reasonably satisfy Controller's regulatory requirements, Controller may conduct an audit:

- Once per calendar year.
- With sixty (60) days' written notice.
- Conducted during business hours, at Controller's expense, and subject to a strict NDA.

9.3. AWS Audits: Controller acknowledges that it cannot physically audit AWS data centers; compliance is instead evidenced by the AWS SOC 3 or SOC 2 Type II reports.

9.4. Exclusions: Nothing in this Agreement will require the Processor to disclose or provide access to: data of other customers, internal

accounting/financial information, trade secrets, or any information that could compromise system security.

10. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The Processor shall provide reasonable assistance to the Company with any data protection impact assessments (DPIAs) and prior consultations with Supervisory Authorities (e.g., GDPR Article 35 or 36, or HIPAA Risk Analysis) solely in relation to the processing of Company Personal Data. Any costs incurred by the Processor in providing such assistance that exceed the provision of existing documentation shall be subject to additional fees, which shall be agreed upon by the Parties in advance and in writing.

11. DELETION OR RETURN OF DATA

11.1. Termination Deletion: Within thirty (30) days following the expiration or termination of the Principal Agreement, the Processor shall delete, and instruct its Sub-processors to delete, all Company Personal Data in its possession or under its control in accordance with its Retention Policy.

11.2. If the Company requires a copy of the Company Personal Data in the Processor's possession, it must request such copy prior to the expiration or termination of the Agreement; requests made after such cessation date will not be considered. Notwithstanding the foregoing, the Processor may retain Company Personal Data to the extent required by Applicable Laws, and only for such period and to the extent mandated by such laws, provided that the Processor ensures the confidentiality of all such Company Personal Data and processes it solely as necessary for the purposes specified in the Applicable Laws requiring its retention, and for no other purpose.

12. DATA TRANSFERS

The Data Controller hereby authorizes the Processor to transfer Company Personal Data across international borders including without limitation from the EEA, Canada, Mexico, Switzerland, and/or the United Kingdom to the United States or Israel, provided that in each case such transfer complies with applicable Data Protection Laws and that the Processor has put in place the necessary safeguards, as required by applicable Data Protection Laws, to facilitate such transfer. Without derogating from the generality of the foregoing, the Processor warrants that where Personal Data is transferred outside of the EEA or the UK, and to the extent required under the Data Protection Laws, it will execute the Standard Contractual Clauses with the recipient of the Personal Data being transferred, unless the processing takes place in a third country or territory recognised by the EU Commission to have an adequate level of protection. The Processor warrants that where required, it will rely on an Adequacy decision or execute Standard Contractual Clauses (SCCs) for processors annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, as may be amended, superseded or replaced;

13. GENERAL TERMS

13.1. Term: This Agreement shall become effective upon execution or acceptance of the Principal Agreement and shall remain in full force until the later of the date when Processor ceases to Process the Company Personal Data or termination of the Principal Agreement. All provisions of this Agreement, which by their language or nature should survive the termination of this Agreement, will survive the termination of this Agreement.

13.2. Notices: All legal notices must be in writing and sent via email. Company notices will be sent to the address associated with its application account. Processor notices shall be sent to: legal@longevity-ai.com.

13.3. Governing Law and Jurisdiction: This Agreement shall be governed by and construed in accordance with the governing law and jurisdiction provisions set forth in the Principal Agreement. In the absence of such provisions, this Agreement shall be governed by the laws of the State of Israel.

13.4. Limitation of Liability: Each Party's liability under this Agreement is subject to the 'Limitation of Liability' provisions set forth in the Principal Agreement. Each Party bears its own investigation costs following a breach unless caused by the other Party's gross negligence.

13.5. Severability: Should any provision of this Agreement be found invalid or unenforceable, the remainder of this Agreement shall remain valid and in full force.

13.6. No Reduction of Obligations. Nothing in this Agreement reduces either Party's obligations under the Principal Agreement in relation to the protection of Company Personal Data.

14. SCHEDULE 1: DETAILS OF PROCESSING

Subject Matter of Processing	AI-driven health management, preventative analytics, and longevity modeling services.
Duration of Processing	The duration of the Principal Agreement plus the 30-day graceful deletion period.
Nature and Purpose of Processing	Predictive disease modeling, medical professional support decision tracking, health trending, optimization of platform functionalities, and patient health lifecycle monitoring.
Categories of Data Subjects	Patients of the Company; Authorized medical staff, clinicians, and practitioners.
Types of Personal Data (PII)	Full Name, Email Address, Date of Birth (DOB), and Gender.
Protected Health Information (PHI)	Medical history, laboratory results, genomic markers, clinical biometric data, and proprietary Longevity AI risk scores.

15. SCHEDULE 2: TECHNICAL & ORGANIZATIONAL MEASURES (TOMs)

The Processor maintains the following technical stack and security controls to meet SOC 2 (Security, Availability, Confidentiality) and HIPAA compliance thresholds:

15.1. Identity & Access Management: Centralized identity provider infrastructure utilizing Google Workspace IDP with Single Sign-On (SSO). Multi-Factor Authentication (MFA) enforcement is mandatory across all systems, including administrative, production environment, and staging access layers.

15.2. Network Security: Production network access is strictly locked and secured via FortiClient VPN utilizing Conditional Access policies to prevent unauthorized endpoint entry.

15.3. Data Encryption Architecture:
• Data at Rest: Encrypted using advanced cryptographic standards (AES-256) powered by AWS Key Management Service (KMS).
• Data in Transit: Encrypted using Transport Layer Security (TLS 1.2 or TLS 1.3) applied universally across all internal and public service endpoints.

15.4. Vulnerability & Posture Management: Automated, continuous application security monitoring via Snyk (covering SAST, DAST, and software dependencies). Infrastructure level compliance and continuous cloud security posture management (CSPM) are validated continuously via Prowler.

15.5. Continuous Penetration Testing: Security postures and threat environments are validated through always-on, AI-agentic penetration testing systems, delivering continuous evaluation of the attack surface.

15.6. Security Logging & SIEM: Centralized system logs, auditing entries, and security events are consolidated via AWS CloudWatch and Graylog SIEM. Critical audit trails and security logs are preserved for a minimum of one (1) year to facilitate forensic investigation and SOC 2 audits.

15.7. Availability & Disaster Recovery: The multi-tenant SaaS environment utilizes multi-AZ (Availability Zone) deployment mechanisms to ensure automated failover capabilities, underpinning an availability matched the service level agreement (SLA). Testing is managed via an annual Incident Response Plan (IRP) review and tabletop exercises.

15.8. Endpoint Protection & MDM: All corporate workstations and remote staff laptops are managed centrally via JumpCloud MDM (Mobile Device Management) and fortified natively with Malwarebytes ThreatDown (EDR/MDR) agents to isolate malware and prevent unauthorized configuration changes.