DATA PROCESSING ADDENDUM TO TERMS OF SERVICE

Effective Date: April 1, 2024

This Data Processing Addendum ("**DPA**") is an addendum to the Terms of Service ("**TOS**") between **SHOEBOX Ltd.**, 301-80 Aberdeen St., Ottawa, ON K1S 5R5 ("**SHOEBOX**" or "**Processor**") and the customer subscribing to the SHOEBOX software, products and services pursuant to the TOS ("**Customer**" or "**Controller**"). The purpose of this DPA is to ensure adequate safeguards with respect to the Processing of Personal Data and the parties agree to comply with the following provisions with respect to Personal Data, each acting reasonably and in good faith.

Five Appendices/Schedules are attached to this DPA and form an integral part of the DPA as they contain the description of the data processing corresponding to the specific products being used:

- Schedule A-1: SHOEBOX® Platform. Comprises modules marketed by SHOEBOX under the names SHOEBOX Remote, SHOEBOX Koalys Remote, SHOEBOX Consult, SHOEBOX Koalys Consult, and SHOEBOX Koalys Confirm.
- Schedule A-2: SHOEBOX® PURETEST
- Schedule A-3: SHOEBOX® ONLINE
- Schedule A-4: SHOEBOX® QUICKTEST

1. DEFINITIONS

All capitalized terms used in the DPA but not defined below have the meaning set out in the TOS.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of an entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data Processed pursuant to this DPA.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA, the Controller is Customer.

"Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed pursuant to this DPA.

"Data Protection Authority" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

"Data Subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

"Personal Data" means any information relating to a Data Subject that is shared with the Processor or acquired, generated or otherwise Processed by the Processor on behalf of the Controller in connection with this DPA.

"Process" shall mean any operation or set of operations which is performed upon Personal Data or sets of Personal Data whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

"Processor" means the entity which Processes Personal Data on behalf of a Controller. For the purposes of this DPA, the Processor is SHOEBOX.

"Sub-processor" means any entity which Processes Personal Data on behalf of a Processor.

2. PROCESSING OF PERSONAL DATA

2.1 Compliance with Applicable Data Protection Laws and Description of the Processing. Both parties agree to comply with Applicable Data Protection Laws regarding Processing Personal Data. The subject matter, duration, purpose and legal basis of the Processing, the types of Personal Data, the categories of Data Subjects Processed under this DPA, as well as the use of cookies and analytics tools, are further specified in Schedules A-1, A-2 etc. for each SHOEBOX software product.

2.2 Controller's Obligations. Controller's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws and acknowledges that Processor is entitled to rely on Controller's instructions in respect of Processing Personal Data. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data. Controllers operating in France are required to implement a health information system in compliance with the PGSSI-S. By accessing the product, Controllers operating in France are providing commitment to comply with the enforceable reference systems of the PGSSI-S.

2.3 Processor's Obligations. All Personal Data Processed by Processor pursuant to the TOS and this DPA is Confidential Information and Processor will Process Personal Data only in accordance with Controller's documented instructions as set forth in the TOS and this DPA, or as otherwise provided by Controller in writing. Processor will not sell the Personal Data Processed under the TOS and this DPA and will not retain, use, or disclose Personal Data outside of the direct business relationship between Processor and Controller, except as required by law or valid and binding order. Where Processor believes that compliance with Controller's instructions would result in a violation of any Applicable Data Protection Laws, Processor shall notify Controller in writing without delay. Processor shall make available to Controller all information necessary to demonstrate Processor's compliance with its obligations under this DPA.

2.4 Processor Assistance Requirements. Processor shall assist Controller with: compliance with Applicable Data Protection Laws; suspected and relevant Data Breaches; notifications to, and inquiries from, a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Controller's obligation to carry out data protection impact assessments and consultations with a Data Protection Authority.

2.5 SHOEBOX Use of Compiled Data. SHOEBOX utilizes an advanced automated system to ensure secure anonymization of Personal Data. This is achieved by employing a combination of suppression, generalization, and/or aggregation techniques. Compiled Data, as defined in the Terms of Service (TOS), is created by transforming the data to a point where individual data subjects cannot be identified. SHOEBOX leverages third-party software, as described in the relevant Schedule A, to perform comprehensive analytics on the Compiled Data SHOEBOX uses and/or combines Compiled Data from across its customer base to: (i) support its customers; (ii) understand how its customers and their Provisioned Users access and use the SHOEBOX software, products and services; (iii) understand the results generated by its customers' use of the SHOEBOX software, products and services; (iv) evaluate how the SHOEBOX software, products and services perform; (v) perform analyses of the Compiled Data,

including but not limited to, analysis of geographic data, demographic data, the number of hearing tests conducted, the number of hearing impairments found, and to identify trends in audiological data; (vi) determine how to make improvements to the SHOEBOX software, products and services and to develop new capabilities; and, (vii) investigate reported bugs in the software and products and identify customers who may be affected by such bugs. Controller hereby agrees that Processor has a royalty-free, worldwide, irrevocable, perpetual right and license to use Compiled Data for the purposes set out in this Section 2.5.

3. NOTIFICATION OBLIGATIONS

3.1 Processor's Notification Obligations. Processor shall immediately notify Controller, in writing, of the following as they relate to Personal Data Processed by Processor on behalf of Controller:

3.1.1 A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;
3.1.2 Any request or complaint received from Controller's employees, patients or participants;
3.1.3 Any question, complaint, investigation, or other inquiry from a Data Protection Authority in respect of Controller's activities pursuant to the TOS or this DPA;
3.1.4 Any request for disclosure of Personal Data that is related in any way to Processor's Processing of Personal Data under the TOS and this DPA;
3.1.5 A Data Breach pursuant to the notification obligations set forth in Section 7.1; and,
3.1.6 Where Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

Processor will assist Controller in fulfilling Controller's obligations to respond to requests relating to Sections 3.1.1 through 3.1.6 above and will not respond to such requests without Controller's prior written consent unless Processor is required to respond by law.

4. CONFIDENTIALITY

4.1 Confidential Information. All Personal Data is Confidential Information.

4.2 Processor's Personnel. Processor will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor will ensure that such confidentiality obligations survive the termination of its respective employment or independent contractor relationship with such individuals. Processor will conduct five-year employment history verification and criminal record checks on all personnel with direct access to Personal Data.

4.3 Limitation of Access. Processor shall ensure that Processor's access to Personal Data is limited to those personnel performing Services in accordance with the TOS and that those personnel only access the minimum necessary amount of Personal Data required to perform the Services.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Controller acknowledges and agrees that Processor and Processor's Affiliates may engage third-party Sub-processors in connection with the provision of the Services. Processor or Processor's Affiliates shall enter into a written agreement with each Sub-processor containing obligations, requirements, and restrictions no less restrictive than those set out in this DPA.

5.2 Notification of Changes to Sub-processors. Processor currently uses the Sub-Processors listed on the applicable Schedule A. Processor will inform Controller of any changes concerning the addition or

replacement of Sub-processors by updating the Sub-processor list on its website. Controller may object to changes in Processor's Sub-processors in good faith but will not unreasonably object to changes to Sub-processors. Controller may terminate the TOS and this DPA if Processor does not satisfactorily address Controller's objections to new Sub-processors to Controller's satisfaction.

5.3 Liability for Acts of Sub-Processors. Processor is fully liable for all of the acts and omissions of its Sub-processors.

6. SECURITY

6.1 Protection of Personal Data. In accordance with Article 32 of the GDPR, the Processor is committed to upholding stringent safeguards to protect the security, confidentiality, and integrity of Personal Data. To gain insight into the specific technical and organizational measures we implement, please visit our security page at https://shoebox.md/security. These measures are designed to prevent unauthorized or unlawful processing, accidental or unlawful destruction, loss or alteration, damage, unauthorized disclosure, or access to Personal Data.

Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

6.2 Audit Rights. Controller, or Controller's designee, has the right to audit and inspect, at Controller's expense, Processor's premises, policies, procedures, and computerized systems via a questionnaire and a one hour remote meeting no more than once per year to make sure Processor complies with the requirements in this DPA. Controller, or Controller's designee, will provide at least 30 days' notification before conducting an audit unless such audit is required due to a Data Breach involving Processor, in which case at least 5 business days' notice is required. Processor will pay for all audits due to a Data Breach involving Processor, Processor's Affiliates, or their Sub-processors. Controller will pay for Processor audit time for audits not related to a Data Breach which exceed the questionnaire and one hour remote meeting. Audits by Controller or Controller's designee will not violate Processor's or Processor's Affiliate's confidentiality obligations.

7. DATA BREACHES

7.1 Data Breach Notification. As a data processor, our primary commitment under the DPA is to support and assist the Controller, in fulfilling its obligations under the GDPR, including Articles 33 and 34. Processor shall notify Controller in writing within 72 hours of discovering a suspected or actual Data Breach, providing all relevant information to facilitate Controller's notification to the supervisory authority as required by Article 33. Processor will also cooperate fully with Controller in fulfilling obligations under Article 34, providing any necessary assistance and information to enable notification of affected individuals if a breach is likely to result in a high risk to their rights and freedoms.

7.2 Data Breach Management. Processor shall make reasonable efforts to identify the cause of a suspected or actual Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach.

8. LIABILITY AND INDEMNIFICATION

8.1 Liability. Processor shall be liable to Controller for direct damages, penalties, fines, costs, losses, liabilities, and fees (including attorneys' and accountants' fees) directly related to a Data Breach that is not caused by Controller.

8.2 Indemnification. Processor will defend, indemnify, and hold Controller harmless from and against all third party claims, actions, demands, or legal proceedings and for all damages, penalties, fines, costs, losses, liabilities, and fees (including attorneys' and accountants' fees) resulting from a Data Breach that is not caused by Controller.

8.3 Limitation of Liability. The limitation of liability sections in the TOS shall apply to this DPA.

9. TERMINATION

9.1 Termination. This DPA shall terminate automatically upon the later of: (a) the termination or expiration of the TOS; or, (b) Processor's deletion of Personal Data. Controller shall further be entitled to terminate this DPA for cause if the Processor is, in the reasonable opinion of Controller, in a material or persistent breach of this DPA.

9.2 Deletion of Data. Within ninety (90) days of the termination of this DPA or upon request, Processor will delete all existing copies of Personal Data unless applicable law requires continued retention of the Personal Data. In instances where local law requires Processor to retain Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data; and will continue to comply with the terms of this DPA.

SCHEDULE A-1

DESCRIPTION OF THE PROCESSING - SHOEBOX® PLATFORM

Description of SHOEBOX Platform

SHOEBOX Platform is an online audiological platform intended for use in conducting hearing testing for diagnosis of possible otologic disorders.

Subject-Matter of the Processing

SHOEBOX processes certain Personal Data listed below on behalf of its customers in relation to hearing testing services.

Duration of the Processing

The duration of processing is the subscription term set out in the applicable invoice.

Nature and Purpose of the Processing

Shoebox is collecting, storing, analyzing, and deleting personal data.

Legal Basis for the Processing

The legal basis for SHOEBOX Processing Personal Data will be one of the following:

- Performance of a contract
- Legitimate business interests
- Compliance with legal obligations

Categories of Data Subjects

- Customers and their Provisioned Users
- Patients or participants whose hearing is being tested

Categories of Data

The Personal Data Processed may concern the following categories of data:

From Customers and/or Provisioned Users:

- Identifying Information
    - Name
    - Email
    - Phone number
    - Last used IP address

From Patients or Participants

- Identifying Information
    - Full Name
    - Date of birth
    - Gender
    - Social Security Number (if enabled for customer)
    - National ID (if enabled for customer)
    - ENT Full Name
    - Notes
    - Phone number
    - Email
    - Address
    - Company / Department OR School / Grade
- Health Data
    - Hearing aid models
    - Audiogram
    - Health information related to hearing testing gathered in questionnaires

Sub-Processors, Purpose and Locations of Processing

Sub-processor	Purpose	Location
Salesforce.com, inc.	Demographics (personal identifiers) are stored on Heroku Shield for USA-based customers. Health data (hearing test results) are stored on Heroku Shield for USA-based customers.	USA
Salesforce.com, inc.	Health data (hearing test results) are stored on Heroku for non-USA-based customers.	Ireland
SIGMA Informatique	Demographics (personal identifiers) are stored on Sigma for non-USA-based customers.	France

Personal data may be accessed from locations outside the EU via data processors.

Any transfer of personal data is subject to an adequacy decision by the EU Commission or appropriate safeguards provided through the EU Commission's standard contractual clauses, cf. article 46 of the GDPR.

SCHEDULE A- 2

DESCRIPTION OF THE PROCESSING - SHOEBOX® PURETEST

Description of SHOEBOX PureTest

SHOEBOX PureTest is an iPad-based audiometer that is used in conjunction with the SHOEBOX Data Management Portal to perform diagnostic hearing testing.

Subject-Matter of the Processing

SHOEBOX processes certain Personal Data listed below on behalf of its customers in relation to hearing testing services.

Duration of the Processing

The duration of processing is the subscription term set out in the applicable invoice.

Nature and Purpose of the Processing

Shoebox is collecting, storing, analyzing, and deleting personal data.

Legal Basis for the Processing

The legal basis for SHOEBOX Processing Personal Data will be one of the following:

- Performance of a contract
- Legitimate business interests
- Compliance with legal obligations

Categories of Data Subjects

- Customers and their Provisioned Users
- Patients or participants whose hearing is being tested

Categories of Data

From Customers and Provisioned Users:

- Identifying and/or Contact Data
    - Customer name
    - Contact information, including postal and email addresses
    - Billing address
    - Billing details (as necessary for our internal accounting purposes and for processing payments through our contracted processing service)
    - Login information for Provisioned Users, such as usernames and encrypted passwords
    - Information about how the Customer and its Provisioned Users use PureTest.
    - Information provided by the Customer and its Provisioned Users to the SHOEBOX support team
- Health Data
    - PureTest biological verification hearing test data for Provisioned Users - stored on the iPad only and not synchronized with the Data Management Portal

From Customer's patients or participants

- Identifying and/or Contact Data
    - Personal
        - Name (first, middle, last name)
        - Gender
        - Date of birth
    - Location details
        - Company
        - School
        - Facility

    - Employment details
        - Employee ID
        - Hire Date
        - Department
        - Job Classification
        - Job Position
        - Status
    - Contact
        - Email Address
        - Home phone number
        - Cell phone number
        - Work phone number
        - Address
    - Health
        - Health Card Number
        - Physician
        - Referring Physician
    - Notes
    - External ID (for imports)

- Health Data Collected When Hearing Tests Performed
    - Audiogram
    - Health information related to hearing testing gathered by questionnaire

From Customer's patients or participants if a Customer subscribes to Audiological Review Services

- Noise surveys, including personal dosimetry with names
- Medical/second opinion reports for clinical determination
- Patient or participant-specific information shared via email and over meetings/calls

Sub-Processors, Purpose and Locations of Processing

Sub-processor	Purpose	Location
Amazon Web Services, Inc.	AWS hosts all customer data within the USA for US-based customers	Virginia, US Northeast
Amazon Web Services, Inc.	AWS hosts all customer data within Canada for non-US-based customers	Canada East (Montreal)

Personal data may be accessed from locations outside the EU via data processors. Any transfer of personal data is subject to an adequacy decision by the EU Commission or appropriate safeguards provided through the EU Commission's standard contractual clauses, cf. article 46 of the GDPR.

Cookies

SHOEBOX PureTest and the SHOEBOX Data Management portal use cookies as follows:

> **Cookies**: Cookies are pieces of information stored directly on the computer that an end user is using. A strictly-necessary cookie is a cookie that is essential for the operation of the software. SHOEBOX PureTest places a strictly-necessary cookie on a Provisioned User's computer to enable that Provisioned User to login and authenticate via Single Sign-On to Customer's identity provider.

SCHEDULE A- 3

DESCRIPTION OF THE PROCESSING - SHOEBOX® ONLINE

Description of SHOEBOX Online

SHOEBOX Online is an online hearing screener that is used in conjunction with the SHOEBOX Data Management Portal to perform hearing screening.

Subject-Matter of the Processing

SHOEBOX processes certain Personal Data listed below on behalf of its customers in relation to hearing screening services.

Duration of the Processing

The duration of processing is the subscription term set out in the applicable invoice.

Nature and Purpose of the Processing

Shoebox is collecting, storing, analyzing, and deleting personal data.

Legal Basis for the Processing

The legal basis for SHOEBOX Processing Personal Data will be one of the following:

- Performance of a contract
- Legitimate business interests
- Compliance with legal obligations

Categories of Data Subjects

- Customers and their Provisioned Users
- Participants whose hearing is being screened

Categories of Data

From Customers and Provisioned Users:

- Identifying and/or Contact Data
    - Customer name
    - Contact information, including postal and email addresses
    - Billing address
    - Billing details (as necessary for our internal accounting purposes and for processing payments through our contracted processing service)
    - Login information for Provisioned Users, such as usernames and encrypted passwords
    - Information about how the Customer and its Provisioned Users use SHOEBOX Online.
    - Information provided by the Customer and its Provisioned Users to the SHOEBOX support team

From Customer's participants

- Identifying and/or Contact Data
    - Name
    - Email address
    - Phone number
    - Location data
    - Age range
    - Gender

- Health Data
    - Hearing screening results

Sub-Processors, Purpose and Locations of Processing

Sub-processor	Purpose	Location
Amazon Web Services, Inc.	AWS hosts all customer data within the USA for US-based customers	Virginia, US Northeast
Amazon Web Services, Inc.	AWS hosts all customer data within Canada for non-US-based customers	Canada East (Montreal)

Personal data may be accessed from locations outside the EU via data processors. Any transfer of personal data is subject to an adequacy decision by the EU Commission or appropriate safeguards provided through the EU Commission's standard contractual clauses, cf. article 46 of the GDPR.

Cookies

SHOEBOX Online and the SHOEBOX Data Management portal use cookies as follows:

> **Cookies**: Cookies are pieces of information stored directly on the computer that an end user is using. A strictly-necessary cookie is a cookie that is essential for the operation of the software. SHOEBOX Online places a strictly-necessary cookie on a Provisioned User's computer to enable that Provisioned User to login and authenticate to the SHOEBOX Data Management Portal.

SCHEDULE A- 4

DESCRIPTION OF THE PROCESSING - SHOEBOX® QUICKTEST

Description of SHOEBOX QuickTest

SHOEBOX QuickTest is an iPad-based hearing screener that is used in conjunction with the SHOEBOX Data Management Portal to perform hearing screening.

Subject-Matter of the Processing

SHOEBOX processes certain Personal Data listed below on behalf of its customers in relation to hearing screening services.

Duration of the Processing

The duration of processing is the subscription term set out in the applicable invoice.

Nature and Purpose of the Processing

Shoebox is collecting, storing, analyzing, and deleting personal data.

Legal Basis for the Processing

The legal basis for SHOEBOX Processing Personal Data will be one of the following:

- Performance of a contract
- Legitimate business interests
- Compliance with legal obligations

Categories of Data Subjects

- Customers and their Provisioned Users
- Participants whose hearing is being screened

Categories of Data

From Customers and Provisioned Users:

- Identifying and/or Contact Data
    - Customer name
    - Contact information, including postal and email addresses
    - Billing address
    - Billing details (as necessary for our internal accounting purposes and for processing payments through our contracted processing service)
    - Login information for Provisioned Users, such as usernames and encrypted passwords
    - Information about how the Customer and its Provisioned Users use QuickTest.
    - Information provided by the Customer and its Provisioned Users to the SHOEBOX support team

From Customer's patients or participants

- Identifying and/or Contact Data
    - Name
    - Email address
    - Phone number
    - Location data
    - Age range
    - Gender

- Health Data
    - Hearing screening information
    - Health information related to hearing screening gathered by questionnaire

Sub-Processors, Purpose and Locations of Processing

Sub-processor	Purpose	Location
Amazon Web Services, Inc.	AWS hosts all customer data within the USA for US-based customers	Virginia, US Northeast
Amazon Web Services, Inc.	AWS hosts all customer data within Canada for non-US-based customers	Canada East (Montreal)

Personal data may be accessed from locations outside the EU via data processors. Any transfer of personal data is subject to an adequacy decision by the EU Commission or appropriate safeguards provided through the EU Commission's standard contractual clauses, cf. article 46 of the GDPR.