INEIRA

Data Processing Agreement

INEIRA Solutions B.V.

Version 1.5
Effective date: 1 October 2026

This Data Processing Agreement ("DPA") forms part of the INEIRA Terms of Service or other agreement governing Customer's use of the INEIRA platform and related services (the "Agreement") between:

a) INEIRA Solutions B.V., with its registered office at Achtseweg Zuid 159R, 5651 GW Eindhoven, the Netherlands, registered with the Dutch Chamber of Commerce under number 99990547 ("INEIRA Solutions", "Processor", "we", "us", "our"), which provides the Services under the product and platform name "INEIRA"; and

b) the entity accepting this DPA ("Customer", "Controller", "you", "your").

This DPA applies where INEIRA Solutions processes Personal Data on behalf of Customer in connection with the Services. Capitalised terms not defined in this DPA have the meaning given to them in the Agreement.

1. DEFINITIONS

1.1 **"Applicable Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under this DPA, including, where applicable, the GDPR and the UK GDPR.

1.2 **"Controller", "Processor", "Personal Data", "Data Subject", "Personal Data Breach", "Processing" and "Supervisory Authority"** have the meanings given to them in Applicable Data Protection Laws.

1.3 **"Customer Personal Data"** means Personal Data included in Customer Data that INEIRA Solutions processes on behalf of Customer under the Agreement.

1.4 **"GDPR"** means Regulation (EU) 2016/679.

1.5 **"UK GDPR"** means the GDPR as incorporated into the laws of the United Kingdom pursuant to the European Union (Withdrawal) Act 2018, as amended.

1.6 **"Security Measures"** means the technical and organisational measures described in Annex 2.

1.7 **"Services"** means the INEIRA platform and related services made available by INEIRA Solutions under the Agreement, including INEIRA Conversation Practice and INEIRA Instructor.

1.8 **"Subprocessor"** means any processor engaged by INEIRA Solutions to process Customer Personal Data.

2. SCOPE AND ROLES

2.1 Subject Matter

INEIRA Solutions provides an AI-supported conversation learning platform (INEIRA) which processes Customer Personal Data in order to provide the Services, including voice-based role-play simulations, interactive lessons based on training content, transcription, scoring, feedback, progress dashboards, analytics, usage measurement, customer support and platform security.

2.2 Roles of the Parties

a) Customer acts as Controller with respect to Customer Personal Data, unless Customer is itself acting as a Processor on behalf of a third-party controller (an "Upstream Controller"), in which case Customer acts as a Processor and INEIRA Solutions acts as a sub-processor.

b) INEIRA Solutions acts as Processor (or sub-processor, as applicable) with respect to Customer Personal Data.

c) Where Customer acts as a Processor on behalf of an Upstream Controller, Customer represents and warrants that it has been duly authorised by the Upstream Controller to appoint INEIRA Solutions as a sub-processor, that the Upstream Controller has agreed to processing terms consistent with this DPA, and that Customer will promptly inform INEIRA Solutions if the Upstream Controller's instructions differ materially from those of Customer under this DPA.

2.3 Customer Instructions

Customer instructs INEIRA Solutions to process Customer Personal Data solely as necessary to provide the Services and as otherwise permitted by the Agreement and this DPA. The configuration of the Services by Customer, including which scores, results and lesson questions are visible to managers and Admin Users, constitutes part of Customer's instructions.

2.4 Details of Processing

The subject matter, nature and purpose of the processing, the categories of Data Subjects and the categories of Personal Data are described in Annex 1.

2.5 No Biometric Processing and No Model Training

INEIRA Solutions does not use voice recordings to create voiceprints or other biometric identifiers and does not use the Services to identify individuals by their voice. INEIRA Solutions does not use Customer Personal Data to train, fine-tune or otherwise improve general AI models, except with Customer's explicit written opt-in or in the form of aggregated and anonymised statistics, as set out in the Terms of Service.

3. PROCESSING ON DOCUMENTED INSTRUCTIONS

3.1 INEIRA Solutions processes Customer Personal Data only on documented instructions from Customer, including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by applicable law. Where INEIRA Solutions is required by law to process Customer Personal Data outside Customer's instructions, INEIRA Solutions will inform Customer of that legal requirement before processing, unless the law prohibits such information.

3.2 INEIRA Solutions will inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws. Customer remains responsible for ensuring that its instructions are lawful.

4. CONFIDENTIALITY

4.1 INEIRA Solutions ensures that persons authorised to process Customer Personal Data are subject to confidentiality obligations, whether by contract or by law, and process Customer Personal Data only as necessary to perform the Services.

5. SECURITY OF PROCESSING

5.1 INEIRA Solutions implements and maintains appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data. INEIRA Solutions operates an information security management system certified under ISO 27001. The Security Measures are described in Annex 2.

5.2 Customer acknowledges that security requirements are relative to the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks to individuals.

5.3 Customer acknowledges that, despite the implementation of appropriate technical and organisational measures, no method of transmission over the internet or of electronic storage is completely secure. INEIRA Solutions does not guarantee that Customer Personal Data will be secure from unauthorised access, loss or alteration, and is not liable for such incidents except as required under Applicable Data Protection Laws or as set out in the Agreement.

6. SUBPROCESSING

6.1 **Authorised Subprocessors.** Customer gives INEIRA Solutions general authorisation to engage Subprocessors to process Customer Personal Data for the purpose of providing the Services. The Subprocessors engaged at the effective date of this DPA are listed in Annex 3.

6.2 **Subprocessor Obligations.** Where INEIRA Solutions engages a Subprocessor, INEIRA Solutions ensures that the Subprocessor is bound by data protection obligations no less protective than those in this DPA, including appropriate confidentiality and security obligations. INEIRA Solutions remains responsible for the performance of its Subprocessors.

6.3 **Changes and Notice.** INEIRA Solutions keeps the list in Annex 3 up to date and makes the current list available on request via legal@ineira.com. INEIRA Solutions will give Customer at least thirty (30) days' prior written notice of any intended addition or replacement of a Subprocessor.

6.4 **Objection Right (applies in the EU and the UK).** Customer may object to a new or replacement Subprocessor on reasonable data protection grounds by notifying INEIRA Solutions in writing within fourteen (14) days of receiving notice under Section 6.3, stating those grounds. If Customer does not object within this period, Customer is deemed to have accepted the new Subprocessor. If Customer objects and the parties cannot resolve the objection in good faith within a further fourteen (14) days, Customer may terminate the affected Services by written notice, without penalty, within thirty (30) days after that period.

7. ASSISTANCE TO CUSTOMER

7.1 **Data Subject Requests.** Taking into account the nature of the processing, INEIRA Solutions provides reasonable assistance to Customer to enable Customer to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Laws. If INEIRA Solutions receives such a request directly, it will refer the Data Subject to Customer.

7.2 **Security and Compliance Assistance.** INEIRA Solutions provides reasonable assistance to Customer with respect to the security of processing, Personal Data Breach notifications, data protection impact assessments and prior consultations with Supervisory Authorities, in each case to the extent required by Applicable Data Protection Laws and taking into account the information available to INEIRA Solutions.

8. PERSONAL DATA BREACH NOTIFICATION

8.1 INEIRA Solutions will notify Customer without undue delay, and where feasible within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

8.2 The notification will include, to the extent available, information about the nature of the Personal Data Breach, the likely consequences, and the measures taken or proposed to address it.

8.3 INEIRA Solutions will cooperate with Customer and provide reasonable assistance to enable Customer to meet its breach-related obligations under Applicable Data Protection Laws.

9. DELETION AND RETURN OF CUSTOMER PERSONAL DATA

9.1 Upon termination or expiry of the Services, INEIRA Solutions will, at Customer's written request and choice, return or securely delete Customer Personal Data, unless applicable law requires retention. Where retention is required, INEIRA Solutions will inform Customer and will not process the retained data for any other purpose.

9.2 Deletion or return will be completed within ninety (90) days of the termination or expiry of the Services, or of Customer's written request, whichever is later, consistent with the retention and backup processes of INEIRA Solutions. INEIRA Solutions will confirm completion in writing.

10. AUDITS AND COMPLIANCE

10.1 INEIRA Solutions makes available to Customer the information reasonably necessary to demonstrate compliance with this DPA.

10.2 Customer may audit compliance with this DPA to the extent required by Applicable Data Protection Laws, subject to the following conditions:

a) audits are limited to once per calendar year, unless a confirmed Personal Data Breach directly affecting Customer Personal Data has occurred, in which case an additional audit may be requested within a reasonable period after the breach;

b) Customer provides at least thirty (30) days' prior written notice, specifying the proposed scope, timing and duration of the audit;

c) the audit is conducted during normal business hours and in a manner that minimises disruption to the operations of INEIRA Solutions;

d) the audit is limited to information relevant to the processing of Customer Personal Data under this DPA;

e) the audit is subject to appropriate confidentiality obligations, and any auditor appointed by Customer signs a confidentiality agreement acceptable to INEIRA Solutions before accessing any systems or information;

f) Customer bears the reasonable costs of the audit, including the reasonable internal costs of INEIRA Solutions and any third-party costs incurred in facilitating it; and

g) INEIRA Solutions may satisfy audit requests in whole or in part by providing its current ISO 27001 certificate and related reports, or other third-party certifications or attestations, where these adequately address the scope of the request.

11. INTERNATIONAL DATA TRANSFERS

11.1 Customer Personal Data is hosted in Microsoft Azure data centres in the Netherlands, Sweden and the United States, as specified in Annex 3. INEIRA Solutions and its Subprocessors may also access Customer Personal Data from other countries where necessary to provide support and maintain the Services.

11.2 Where Applicable Data Protection Laws require safeguards for international transfers, INEIRA Solutions implements appropriate safeguards to lawfully transfer Customer Personal Data.

11.3 **EU transfers (applies in the EU).** Where the GDPR applies and Customer Personal Data is transferred outside the European Economic Area, the transfer is based on an adequacy decision of the European Commission (including the EU-US Data Privacy Framework for certified recipients) or on the Standard Contractual Clauses adopted by the European Commission.

11.4 **UK transfers (applies in the UK).** Where the UK GDPR applies and Customer Personal Data is transferred outside the United Kingdom, the transfer is based on UK adequacy regulations or on the UK International Data Transfer Addendum to the Standard Contractual Clauses.

12. CUSTOMER RESPONSIBILITIES

12.1 Customer represents and warrants that it has complied and will comply with Applicable Data Protection Laws in relation to Customer Personal Data, including that it has a lawful basis to collect, use and disclose Customer Personal Data to INEIRA Solutions for processing.

12.2 Customer is responsible for informing Users and other Data Subjects about the processing of their Personal Data in the Services, including the use of AI, the recording and scoring of practice sessions, and the information visible to managers and Admin Users.

12.3 Customer is responsible for determining whether the Services are appropriate for its compliance requirements, including which Customer Personal Data it submits to the Services, and will not submit Personal Data that is prohibited under the Agreement or that requires heightened protection unless expressly agreed in writing.

13. LIABILITY

13.1 Liability arising under this DPA is subject to the limitations of liability set out in the Agreement, unless Applicable Data Protection Laws require otherwise.

14. CONFLICT AND ORDER OF PRECEDENCE

14.1 In the event of a conflict between this DPA and the Agreement regarding the processing of Customer Personal Data, this DPA prevails. Where the Standard Contractual Clauses apply, they prevail over this DPA.

15. TERM AND TERMINATION

15.1 This DPA remains in effect for as long as INEIRA Solutions processes Customer Personal Data on behalf of Customer under the Agreement.

16. GENERAL

16.1 **No Third-Party Beneficiaries.** This DPA does not confer any rights on any third party, unless required under Applicable Data Protection Laws.

16.2 **Changes.** INEIRA Solutions may update this DPA to reflect changes in laws, regulations or the Services. If changes are material, INEIRA Solutions will provide reasonable notice. Changes will not reduce the level of protection of Customer Personal Data.

16.3 **Governing Law.** This DPA is governed by the law and jurisdiction set out in the Agreement, unless Applicable Data Protection Laws require otherwise.

ANNEX 1: DETAILS OF PROCESSING

A. Subject Matter

Provision of the Services to Customer, including voice-based conversation practice, interactive lessons, transcription, scoring, feedback, progress dashboards, analytics, usage measurement, customer support and platform security.

B. Duration of Processing

For the duration of the Agreement, plus the period for deletion or return described in Section 9 and the retention and backup cycles of INEIRA Solutions.

C. Nature and Purpose of Processing

Processing necessary to provide the Services, including collecting, recording, transcribing, organising, storing, analysing and scoring practice sessions, generating training outputs and lessons, measuring usage, providing support, preventing abuse and ensuring security.

D. Categories of Data Subjects

As determined by Customer, these may include:

- Customer's employees and contractors;
- Customer's trainees, agents, managers and administrators;
- Customer's customers and prospects, where included in training materials or scenarios; and
- other individuals whose Personal Data is included in Customer Data.

E. Categories of Personal Data

As determined by Customer, these may include:

- name, email address, role and user identifiers;
- voice recordings and audio content;
- transcripts, messages, prompts, questions asked during lessons and scenario inputs;
- scores, feedback, progress levels and other training results;
- training materials uploaded by Customer, including documents, images and video;
- usage data and interaction metadata; and
- support communications.

F. Special Categories of Personal Data

Not intended to be processed. Customer will not submit special categories of Personal Data unless expressly agreed in writing and appropriately safeguarded. Voice recordings are not processed for the purpose of uniquely identifying a natural person.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

INEIRA Solutions maintains a risk-based information security programme within an information security management system certified under ISO 27001. The Security Measures include:

1. Access Control

- role-based access control;
- least privilege principles; and
- strong authentication for administrative access.

2. Data Protection

- encryption in transit (TLS);
- encryption at rest; and
- logical segregation of customer environments where applicable.

3. Logging and Monitoring

- security logging for critical systems; and
- monitoring for suspicious activity where feasible.

4. Incident Response

- documented incident response and escalation procedures; and
- breach assessment and notification processes, including notification to Customer within seventy-two (72) hours where feasible.

5. Availability and Resilience

- backups and recovery procedures; and
- measures to maintain service availability.

6. Personnel Security

- confidentiality obligations for all personnel; and
- security awareness training.

7. Vendor Management

- due diligence on Subprocessors; and
- contractual safeguards for Subprocessors.

ANNEX 3: SUBPROCESSORS

At the effective date of this DPA, INEIRA Solutions engages the following Subprocessor for the processing of Customer Personal Data:

Subprocessor	Purpose of processing	Processing locations
Microsoft (Microsoft Ireland Operations Limited and its affiliates), Microsoft Azure	Cloud hosting and storage of the platform, and access to AI models through Azure OpenAI Service for simulations, lessons, transcription, scoring and feedback	The Netherlands, Sweden and the United States

Changes to this list are notified in accordance with Section 6.3.

END OF DATA PROCESSING AGREEMENT