AIHR MODEL DATA PROCESSING AGREEMENT

Version June 2025

This Data Processing Agreement (hereinafter: "Agreement") is entered into by and between:

Controller
_____ (Customer name, address)
(hereinafter referred to as "Controller")

Processor
AIHR B.V. Weena 690, 3012 CN Rotterdam, the Netherlands
(hereinafter referred to as "Processor")

Each a "Party," and collectively the "Parties."

Whereas:

a) On _____ (date), the Parties formed the _____ (title of the main contract), hereinafter: 'Main Contract', under which the Processor will provide services to the Controller;
b) As part of the performance of the Main Contract, the Processor will Process Personal Data for the Controller;
c) The processing of Personal Data by the Processor is governed by the General Data Protection Regulation (GDPR);
d) In the present data processing agreement ('Data Processing Agreement'), the Parties wish to set out the following arrangements, in addition to the GDPR, concerning the Processing of Personal Data;

Agree as follows:

Article 1 Definitions

1.1 Terms used in the Data Processing Agreement that are defined in the GDPR carry the same meaning as defined there. All other capitalized terms used in this document have the same meaning as the definitions within the General Terms and Conditions B2B of AIHR.
1.2 **Annexes**: attachments to the Data Processing Agreement that are an intrinsic part of the Data Processing Agreement.

Article 2 Effective date and duration

2.1 Unless the Parties agree otherwise, the Data Processing Agreement comes into effect when the Contract is formed.
2.2 The Data Processing Agreement terminates at the moment that the Processor finishes Processing Personal Data under the Contract and the arrangements concerning the return and/or erasure of Personal Data have been fulfilled.

Article 3 Subject of the Data Processing Agreement

3.1 The Processor will Process the Personal Data made available by or via the Controller only as required by the Controller for the purposes of performing the Contract, including by automated means, and only in accordance with the Controller's written instructions, unless the Processor is obliged to Process the Personal Data in accordance with an applicable law. Where this applies, before proceeding to Process the Personal Data, the Processor will notify the Controller accordingly, unless that law prohibits such notification by reason of important grounds of public interest.
3.2 The Processing procedures to be carried out by the Processor are described in Annex 1.
3.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes this GDPR or other applicable law.

Article 4 Substantive arrangements

4.1 **Security measures**
The Processor will have appropriate technical and organisational measures in place to properly secure the Personal Data, as described in Article 32 of the GDPR. The technical and organisational measures are further described in the Information Security Statement.

4.2 **Audits**
Processor acknowledges and agrees that Controller may, upon providing at least one month's written notice, nominate a reputable third-party - bound by strict confidentiality obligations - to audit Processor's relevant records to verify compliance with this Data Processing Agreement. No more than one audit may be conducted in any 12-month period, and only in case of a material breach of this Data Processing Agreement is reasonably suspected. The Processor reserves the right to reasonably object to the nominated auditor and request an alternative third party. Audits shall be conducted during normal business hours and in a manner that does not unreasonably interfere with Processor's operations. The costs of such audits, including both the Controller's expenses and any costs incurred by Processor, shall be borne by the Controller.

4.3 **Processing outside the EEA**
The Processor may Process (or give instructions to Process) Personal Data outside the European Economic Area if the conditions laid down in Articles 45 or 46 of the GDPR are satisfied. The Processor shall notify the Controller before any instance of Processing outside the EEA.

4.4 **Confidentiality**
Persons working for the Processor (or a Sub-processor) and the Processor (or Sub-processor) itself must treat the Personal Data with which they work as Confidential Information. Accordingly, the persons working for the Processor and Sub-processors have signed non-disclosure agreements, or are otherwise bound in writing by the confidentiality obligation.

4.5 **Sub-processors**
The Processor will list the Sub-processors that are known at the time of forming the Data Processing Agreement in Table 3 of Annex 1. The Controller hereby gives its general consent for engaging the services of Sub-processors. Once the work has commenced, the Processor will inform the Controller of any plans to engage the services of new Sub-processors. The Controller has the right to object to the engagement of new Sub-processors on reasonable grounds relating to the protection of Personal Data within 30 days of notification. In case of such an objection, we will discuss concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-processor, or permit you to suspend or terminate the affected (part of the) Service in accordance with the termination provisions of the Contract without liability to either party. Where we engage Sub-processors, we will impose data protection terms on the Sub-processors that provide at least the same level of protection for Personal Data as those in this Data Processing Agreement. We will remain responsible for each Sub-processor's compliance with the obligations within this document.

4.6 **Data Subject rights**
If a Data Subject invokes his or her rights as described in Articles 12 to 22 of the GDPR, the Processor will help the Controller upon request to make a decision on those rights within the time prescribed by law.

4.7 **Data Protection Impact Assessments and Prior Consultation**
Whenever the Data Controller so requests, the Processor will cooperate in a Data Protection Impact Assessment (DPIA) and prior consultation, as described in Articles 35 and 36 of the GDPR.

Article 5 Personal Data Breaches

5.1 If the Processor identifies or suspects a Personal Data Breach, it will report this to the Controller without undue delay, but no later than within 48 hours. The Processor will report, in so far as this is known, the presumed cause of the Breach or suspected Breach, the category of Personal Data, the category of Data Subjects and the number of Data Subjects.

5.2 In the event of a Breach, the Processor will take all measures without undue delay to remedy the Breach, minimize the consequences and prevent further Breaches.

5.3 The Processor will keep a detailed log of the Breaches and the measures taken in response to Breaches. The Controller will be given access to that log if and when it so requests.

5.4 The Controller will decide whether the Breach must be notified to the supervisory authority

and/or the Data Subject. The Processor will give the Controller whatever support is necessary in connection with the notification to the supervisory authority and/or the Data Subject.

Article 6 Liability

6.1 Any limitations of liability agreed in the Contract also extend to this Data Processing Agreement.

Article 7 Termination of the Data Processing Agreement

7.1 In case of termination of the Contract, the Controller has the right to request the return or deletion of Personal Data. In any case the Processor did not receive such a request, the Processor shall delete all Personal Data of the Controller within 1 year after termination.

Article 8 Other provisions

8.1 This agreement is governed by Dutch law. Any and all disputes, including disputes that only one Party considers to be such, in the first instance will be referred to the competent court specified in the Contract.

Signatures
Agreed and signed,

Controller Company	Processor
_____	_____
Company name: _____	Company name: AIHR B.V.
Represented by: _____	Represented by: Erik van Vulpen (Director)
Signed on: _____	Signed on: _____
Place: _____	Place: Rotterdam

Annex 1: List of personal data to be processed

1. Name of Processing procedure, purposes, categories of Data Subjects, categories of Personal Data and where applicable transfers to third countries

Name of Processing procedure	**Purposes of Processing**	**Categories of Data Subjects**	**Categories of Personal Data (including special categories of Personal Data)**
Members	Transfer personal data from members of courses to AIHR	Employees of Client	Name, email
Access	Giving Members access to courses	Members of Client	Name, email
Report	Reporting progress to Clients	Employees / Members of Client	Name, certificate program, learning progress, total time learning, last activity, learning streams, exam scores (possibly)

2. Contact details

Liaison officer at the Data Controller	Name: _____ Contact details: _____
Liaison officer at the Data Processor	Name: Erik van Vulpen Contact details: legal@aihr.com

Note: If the information in the tables above changes, the Parties must notify each other as soon as possible.

3. Sub-processors

Sub-processor's name and contact details	**Location**	**Outsourced Processing procedures**	**Application**	**Data residence**
Amazon Web Services (AWS) Inc	410 Terry Avenue North, Seattle, WA 98109-5210, USA	Scalable virtual servers for running applications in the cloud.	LMS	EEA
Auth0	100 1st St Suite 150, San Francisco, USA	User identities, authentication logs, session data, configuration settings.	LMS	EEA
Bettermode	22 Wellesley Street East, 1607, Toronto, Canada	User-generated content, member profiles, discussion threads, engagement metrics.	Community	EEA
Google Ireland Limited	Gordon House, Barrow Street Dublin 4, Ireland	Gemini 2.5 Flash processes full conversation transcripts for AI Roleplays and saves them in Google Cloud.	AI Roleplay (optional)	US
Elevenlabs Ltd.	169 Madison Ave #2484 New York, NY, 10016, USA	AI Voice generator, speech to text, text to speech	AI Roleplay (optional)	US

GDPR Appropriate safeguards: with Sub-processors located outside the European Economic Area we concluded Standard Contractual Clauses. Furthermore, the Sub-processors in the USA have reliable mechanisms for personal data transfers from the EU, UK and Switzerland, based on the Data Privacy Framework.