Zebrain Data Processing Agreement

Version: 2025.11.03

This Data Processing Agreement (“DPA”) is incorporated into and forms an integral part of the Framework Agreement (“Agreement”) between:

- Zebrain AB (“Supplier”), and
- [Customer Name] (“Customer”).

1. Definitions

For this DPA, the following terms have the meanings given below (and all terms defined in the Agreement and applicable Data Protection Laws have the same meaning):

- “Data Protection Laws” means all applicable laws regarding the protection of personal data, including the GDPR.
- “Personal Data” means any information relating to an identified or identifiable natural person.
- “Processing” means any operation performed on Personal Data, as defined in the GDPR.
- “Sub-processor” means any processor engaged by Supplier to process Personal Data on behalf of Customer.
- ”Instructions” means written instruction from Customer regarding the processing of personal data under this DPA

For the avoidance of doubt, individual coaches and consultants engaged by Zebrain to deliver services within the Zebrain platform act under Zebrain’s responsibility and instructions. They are not considered Sub-processors under this DPA.

2. Priority of Terms

In the event of any conflict or inconsistency between this Data Processing Agreement and the Framework Agreement, the provisions of this Data Processing Agreement shall prevail with respect to all matters relating to the processing of Personal Data. For any data protection-related issues, this DPA is controlling to ensure compliance with applicable Data Protection Laws.

3. Scope, purpose and instructions

Supplier will process Personal Data solely. in accordance with this DPA, the Agreement, and Customer’s written instructions as set out in the appendix ”Instructions to DPA”.

4. GDPR Compliance

Zebrain commits to keep fully aligned with the General Data Protection Regulation (GDPR). We undertake to implement all requisite technical and organizational measures to protect Personal Data, and our Platform and associated processes will stay designed to meet or exceed GDPR standards for security, privacy by design, and lawful processing.

5. Roles

5.1 Customer as Data Controller

The Customer is the Data Controller and determines the purposes and means of Processing, for data provided both by the Customer and by its users

5.2 Zebrain as Data Processor (Platform Data)
Any Personal Data that is directly entered, generated, or otherwise provided by Customers users via the Platform—such as during registration, feedback, or coaching sessions—is processed by Zebrain in its capacity as Data Processor in accordance with appendix ”instructions to DPA”

6. Data Processing

When Zebrain processes Personal Data on behalf of the Customer, Zebrain shall:

- Process such Personal Data only according to the Customer’s documented instructions.
- Assist the Customer in responding to Data Subject requests (access, rectification, erasure, etc.).
- Maintain records of processing activities and provide these records upon the Customer’s request.
- No Processing for Own Purposes: Zebrain shall not process any Personal Data for its own purposes or for any purposes beyond those expressly defined in the Customer’s documented instructions. Any processing outside these instructions is strictly prohibited unless the Customer provides explicit, written authorization.
- Zebrain shall assist the Controller in ensuring compliance with Articles 32–36 of the GDPR, including security of processing, breach notification, data-protection impact assessments, and prior consultations with supervisory authorities.

7. Data Security

Supplier shall implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of Personal Data. These measures meet or exceed industry standards. A detailed description of these measures is available upon request.

Supplier shall ensure privacy by design and by default measures in accordance with GDPR Article 25, including implementing technical and organizational measures from the outset to protect privacy.

8. Confidentiality

The Processor shall ensure that all persons authorized to process Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality. The obligation shall survive termination of employment or contract. Authorized personnel shall process Personal Data only on instructions from the Controller, unless required to do so by Union or Member State law.

9. Sub-processors

9.1 General Authorization & Notice
The Processor is authorized to engage Sub-Processors for the Processing of Personal Data under this DPA, provided it notifies the Controller in writing at least thirty (30) days before adding or replacing any Sub-Processor. The notice must include the name of the proposed Sub-Processor, the nature of the Processing activities, and the location(s) where those activities will be carried out.

9.2 Right to Object
If the Controller has reasonable grounds related to data protection to object to the proposed Sub-Processor, the Controller shall provide written notice of such objection within thirty (30) days of receiving the Processor’s notice. The Parties shall then endeavor in good faith to resolve the objection within the same thirty (30)-day period.

9.3 Termination for Sub-Processor Objections

If the Parties fail to resolve the Controller's objection within thirty (30) days of the objection notice, the Controller may terminate the affected portion of the services without incurring any penalty or additional cost. Such termination shall not affect any accrued rights or obligations under this DPA or the Agreement.

9.4 Sub-Processor Agreements:
The Processor shall enter into written agreements with each Sub-Processor, imposing obligations no less protective than those set out in this DPA. Each Sub-Processor must, in particular, maintain appropriate technical and organizational measures to safeguard Personal Data in accordance with Data Protection Laws.

9.5 Liability
The Processor remains fully liable to the Controller for the performance of its Sub- Processors' obligations under this DPA.

9.6 Record-Keeping
Upon the Controller's request, the Processor shall promptly provide or make available an updated list of Sub-Processors, including their names, locations, and the nature of their Processing activities.

10. Data Transfers

Personal Data shall remain processed primarily in the EU/EEA. Transfers outside the EU/EEA will occur only when appropriate safeguards (e.g., Standard Contractual Clauses or equivalent) are in place. For transfers outside the EU/EEA, the Supplier relies on either the EU Commission Implementing Decision (EU) 2021/914 contractual clauses (SCCs) or, where applicable, on the Data Privacy Framework to ensure an adequate level of protection. Additionally, the Supplier (and its Sub-Processors) will perform Transfer Impact Assessments (TIA) as necessary to assess and mitigate any risks associated with such transfers.

11. Data Breach

Supplier shall notify the Customer of a Personal Data breach without undue delay and, in any event, no later than 48 hours after becoming aware of the breach. Such notification shall include:

- The nature and scope of the breach,
- It's likely consequences, and
- The measures taken or proposed to address the breach.

If circumstances prevent the Supplier from providing a complete notification within 48 hours, the Supplier shall provide an initial notification with available information and supplement it as furthers details become known.

12. Term and Termination

12.1 Duration
This DPA shall remain in effect for the same term as the underlying Agreement and shall automatically terminate upon the expiration or termination of the Agreement, unless otherwise required by applicable law.

12.2 Post-Termination Obligations (Processor Data)
Upon termination or expiration of the Agreement, and at the Controller's written direction, Zebrain will securely delete or, if technically feasible and agreed upon by both Parties, anonymize any Personal Data that Zebrain processes in its capacity as Data Processor, unless retention is required by law. Zebrain shall complete such deletion or anonymization within thirty (30) days of receiving the Controller's instructions. Zebrain ensures secure, irreversible deletion or anonymization consistent with industry standards (e.g., NIST 800-88 or equivalent) so that data cannot be reconstructed.

12.3 Deletion Confirmation
If requested in writing by the Controller, Zebrain shall provide confirmation that such deletion of Personal Data has been completed in accordance with this Section.

12.4 Survival
Any provisions in this DPA related to confidentiality, liability, or other obligations intended to survive termination shall remain in effect after termination of the Agreement.

13. Audit Rights & Inspection Protocol

The Processor shall maintain adequate documentation to verify its compliance with this DPA and applicable Data Protection Laws.

The Controller, or a third party approved by the Processor, may conduct audits, provided that the Controller gives at least 60 days' written notice and that any audit is conducted during normal business hours in a manner that minimizes disruption to the Processor's operations.

Audits shall be strictly limited to verifying compliance with this DPA and applicable Data Protection Laws and shall not extend to reviewing any unrelated operational or commercial information. For clarity, such audits shall be limited solely to aspects directly related to the processing of Personal Data under this DPA. The Processor shall provide necessary assistance and reasonable access to relevant documentation and, if required, its Processing facilities, subject to mutually agreed conditions. Each Party shall bear its own costs associated with any audit or inspection, and the Processor shall not incur any additional liabilities beyond those expressly set out in this DPA.

Notwithstanding the general 60-day notice period, in the event of a confirmed
Personal Data breach or other security incident that materially impacts the Processing of Personal Data under this DPA, the Controller may request an audit on shorter notice. The Parties shall work in good faith to agree on a reasonable timeframe and scope that addresses the incident while minimizing operational disruption.

14. Liability and Indemnification

14.1 Indemnification by the Processor
If the Processor processes Personal Data in breach of (i) the Controller's lawful instructions, (ii) this DPA, or (iii) applicable Data Protection Laws, and such breach directly causes a loss, penalty, or damage to the Controller, the Processor shall indemnify the Controller for the direct and actual losses or penalties incurred as a result of that breach. This indemnification applies only to losses attributable solely to the Processor's proven breach and does not cover any failure or omission by the Controller or any third party outside the Processor's control.

14.2 Conditions for Indemnification
In the event of any regulatory action, claim, or complaint by a Data Subject or supervisory authority:

- The Controller shall promptly notify the Processor in writing, providing all relevant details of the claim or action;
- (b) The Processor shall have the opportunity, at its own expense, to comment on any proposed defense or settlement, provided that such involvement does not adversely affect the Controller's defense; and
- (c) The Controller shall use reasonable efforts to mitigate any damages and avoid or reduce penalties or losses related to the claim or action.

14.3 Exclusions and Limitations

Except as required by law, neither Party shall be liable for any indirect, incidental, consequential, special, or punitive damages arising under this DPA. The Processor's total liability under this DPA shall be subject to any overall liability caps or limitations set forth in the Framework Agreement, unless otherwise mandated by applicable law.

15. Governing Law and Dispute Resolution

This DPA shall be governed by and construed in accordance with the governing law specified in the Agreement. Any disputes arising out of or relating to this DPA shall be resolved in accordance with the dispute resolution procedures set forth in the Agreement.

16. Amendments

Any amendments or changes to this DPA must be made in writing and signed by both Parties.

Appendix 1 – Instructions to the Data Processing Agreement

Version: 2025.10.10

These Instructions constitute an integral part of the Data Processing Agreement entered between [the Customer, Data Controller] ("Controller") and Zebrain AB ("Processor").

1. Purpose of Processing

The personal data shall be processed to enable the Controller to:

- Provide employees with access to Zebrain's digital platform for people development.
- Support employees in their individual development.
- Enable the follow-up, measurement, and analysis of the implementation and effectiveness of development initiatives.
- Provide managers and HR personnel with insights for the purpose of monitoring investments in competence development.

2. Categories of Data Subjects

- Employees of the Controller who use the platform.
- Managers, supervisors, or HR personnel of the Controller with administrative access.
- (Where applicable) external coaches associated with users act under Zebrain's responsibility and instructions. They are bound by written confidentiality and data-protection undertakings equivalent to those applicable to Zebrain personnel.

3. Categories of Personal Data

- **Identity and contact details:** name, email address, user ID.
- **Organizational information:** department, role, manager/employee relationships.
- **User data:** activity on the platform, e.g., responses to self-assessments, feedback, goals.
- **Communication data:** chats, bookings, meeting notes recorded within the platform.
- **Technical logs:** login data, usage statistics.

4. Legal Basis for Processing

The Controller instructs that the legal basis for the processing shall be one or more of the following, depending on the context of use:

- **Legal obligation:** the employer's duty to provide competence development.

- **Legitimate interest:** the employer's interest in developing employee skills and performance.
- **Contract:** where applicable, if the employee independently enters into an agreement to use the platform.

5. Duration of Processing

Personal data shall be processed for as long as the user remains active on the platform.

Upon termination of use, the data shall be deleted or anonymized in accordance with the agreed retention procedures and in line with the Data Processing Agreement and Privacy Notice. *(The standard retention period is 12 months, unless otherwise agreed.)*

5a. Transfers outside the EU/EEA

The Processor shall not transfer Personal Data outside the EU/EEA without the Controller's prior written authorization and only where appropriate safeguards under Chapter V of the GDPR (such as Standard Contractual Clauses or adequacy decisions) are in place.

6. Instructions to Zebrain AB (Processor)

- Zebrain shall process personal data under this DPA solely in accordance with the DPA and these Instructions
    - Zebrain shall not process personal data under this DPA for its own purposes.
    - Zebrain shall assist the Controller in fulfilling obligations under the GDPR, including data subject rights.
    - Zebrain shall maintain appropriate (clear and usable) instructions and procedures for practical fulfillment of data subject requests pertaining to GDPR Articles 15-18, 21
    - Zebrain shall take appropriate measures to be able to notify the Controller without undue delay upon discovery of a personal data breach under this DPA.
    - Zebrain shall assist the Controller in fulfilling its obligations according to the GDPR Article 13, by making a privacy notice related to this DPA available to end users through its platform.

The Controller remains solely responsible for compliance with its information obligations under the GDPR. Zebrain's role is limited to providing visibility of the Privacy Notice within the platform on behalf of the Controller.

- Zebrain shall, through its product interfaces, keep end users reminded of their obligation to not enter sensitive business data or directly identifiable personal data

Appendix 2 - Sub-Processors

Version: 2026.02.04

Recipients who we share personal data with

For the purposes set out we may transfer your personal data to our sub-processors in the European Union, such as IT providers (e.g. for operations, technical support and maintenance of IT systems and provider of video solution in our platform) and others who provides services on our behalf. These parties will generally act as sub-processors relating to the processing of personal data, which means that they are contractually obliged to process your personal data only on behalf of and in accordance with our Customers instructions. They are also required by law and agreement to take appropriate technical and organizational security measures to protect your data.
We otherwise share personal data as follows.

Purpose
For internal administration, reporting and external business purposes.

Legal basis
We base the processing on our legitimate interest to run our business in an efficient manner (Art. 6 (1) (f) GDPR).

List of Sub-processors, Their Roles, and Contact Details

1. Amazon Web Services (AWS)

• Role: Cloud computing and data management
• Services Provided: Compute, storage, database, and other cloud services.
• Location of Data Processing: Sweden
• Address: Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109, USA
• Website: aws.amazon.com
• Compliance and Security Information: AWS Compliance

2. Microsoft Azure

• Role: Compute, storage, database, and other cloud services. ChatGPT is used via Azure.
• Services Provided: Cloud computing, storage, and data management services.
• Location of Data Processing: Sweden
• Address: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA
• Website: azure.microsoft.com
• Compliance and Security Information: Microsoft Compliance

3. Okta

• Role: Identity and access management
• Services Provided: Identity and access management services.
• Location of Data Processing: Germany
• Address: Okta, Inc., 100 First Street, San Francisco, CA 94105, USA
• Website: okta.com
• Compliance and Security Information: Okta Trust and Compliance

4. Sentry

• Role: Application monitoring and error tracking
• Services Provided: Application monitoring and error tracking services.
• Location of Data Processing: Germany

• Address: Sentry, 45 Fremont Street, San Francisco, CA 94105, USA
• Website: sentry.io
• Compliance and Security Information: Sentry Security

5. Sendgrid

• Role: Mail delivery platform
• Services Provided: Send mails from the Zebrain platform to clients
• Location of Data Processing: Germany and Ireland
• Address: Sendgrid, Inc., 1801 California Street Suite 500, Denver, Colorado 80202, USA
• Website: sendgrid.com
• Compliance and Security Information: Sendgrid Security

6. OpenAI
• Role: AI
• Services Provided: API for AI queries
• Location of Data Processing: European Union
• Address: 1455 3rd Street, San Francisco, CA 94158, USA
• Website: openai.com
• Compliance and Security Information: https://trust.openai.com/

7. Google Gemini
• Role: AI
• Services Provided: API for AI queries
• Location of Data Processing: European Union
• Address: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
• Website: https://gemini.google/about/
• Compliance and Security Information: https://cloud.google.com/trust-center

8. Mistral
• Role: AI
• Services Provided: API for AI queries
• Location of Data Processing: European Union
• Address: Mistral AI, 15 rue des Halles, 75001 Paris, France
• Website: https://mistral.ai/
• Compliance and Security Information: https://trust.mistral.ai/

9. Anthropic
• Role: AI
• Services Provided: API for AI queries
• Location of Data Processing: European Union
• Address: 500 Howard Street, San Francisco, CA 94104, USA
• Website: https://www.anthropic.com/
• Compliance and Security Information: https://trust.anthropic.com/