



DATA PROCESSING ADDENDUM

Version 2

Published: 2026-10-21

This Data Processing Addendum ("DPA") forms part of the Agreement between ****Innerspace GmbH**** ("Processor") and the customer entity entering into the Agreement for the use of the Services ("Controller"), as defined in the Innerspace General Terms and Conditions ("GTC").

This DPA applies to the extent that the Processor processes Personal Data on behalf of the Controller in connection with the Services and forms an integral part of the Agreement, including the Innerspace General Terms and Conditions.

Order of Precedence

In the event of any conflict between this DPA and the Agreement, including the Innerspace General Terms and Conditions (GTC), the provisions of this DPA shall prevail solely with respect to the processing of Personal Data. In all other respects, the terms of the Agreement shall remain unaffected and continue to apply.

Definitions

Capitalised terms not defined in this DPA have the meaning given in the Agreement or the GTC.

For the purposes of this DPA, the following terms have the meanings set out below.

GDPR refers to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Personal Data means any information relating to an identified or identifiable natural person.

Processing refers to any operation or set of operations performed on Personal Data, including collection, storage, use, disclosure or deletion.

Controller means the entity that determines the purposes and means of the processing of Personal Data.

Processor means the entity that processes Personal Data on behalf of the Controller.

Sub-processor means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

Subject Matter and Duration of Processing

The Processor shall process Personal Data solely for the purpose of providing the Services under the Agreement and only on documented instructions from the Controller, unless the Processor is required to process Personal Data by Union or Member State law to which the Processor is subject. Processing shall generally continue for the duration of the Agreement, subject to any legal obligations requiring the Processor to retain certain information for a longer period.

Nature of Processing and Purpose of Processing

Nature of Processing. In the course of providing the Services, the Processor performs processing operations necessary for the technical operation of the Innerspace platform. These operations may include the hosting and storage of data within the platform environment, the organisation and retrieval of information, the transmission of data within the system, the maintenance of operational and security logs, and the provision of technical support and system maintenance activities.

Purpose of Processing. The purpose of such processing is to enable the delivery and operation of the Services for the Controller. This includes the administration of user accounts, the delivery of digital training content, the recording and analysis of training progress and performance metrics, the maintenance of platform security and integrity, and the provision of customer support related to the Services.

Categories of Data Subjects

Depending on the way the Controller uses the Services, Personal Data processed under this DPA may relate to employees, trainees, contractors, administrators, platform users, or other individuals whose Personal Data is submitted to the Services by or on behalf of the Controller.

Types of Personal Data

Personal Data processed within the Services may include following information:

- Names and E-Mails
- Training records

The following data will only be generated and processed on explicit instruction by the Controller:

- Photos with persons and equipment
- Video recordings with personnel and equipment

The Controller determines which Personal Data is submitted to and processed within the Services.

Unless otherwise expressly agreed in writing between the parties, the Services are not intended to process special categories of personal data within the meaning of Article 9 GDPR, including health data, biometric data, or similar sensitive information. The Controller shall not submit such data to the Services unless the parties have expressly agreed on appropriate safeguards and processing conditions in accordance with applicable data protection law.

Processor Obligations

The Processor shall process Personal Data only on documented instructions of the Controller and solely for the purpose of providing the Services. The parties agree that the Controller's use of the Services, including the configuration of the platform and submission of Personal Data to the Services, constitutes documented instructions to the Processor for the purposes of this DPA. Any additional instructions shall be provided in documented form by the Controller. The Processor may refuse to follow instructions that are unlawful or that fall outside the scope of the Services.

The Processor shall ensure that persons authorised to process Personal Data are bound by appropriate confidentiality obligations and receive appropriate training regarding data protection and information security. Furthermore, the Processor shall implement appropriate technical and organisational measures to safeguard Personal Data and shall provide reasonable assistance to the Controller in fulfilling obligations under Articles 32 to 36 GDPR where relevant. The Processor shall also assist the Controller in responding to requests from data subjects exercising their rights under applicable data protection law.

Confidentiality

The Processor shall ensure that all persons authorised to process Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. Access to Personal Data shall be restricted to those personnel who require such access for the performance of their duties.

Technical and Organisational Measures

The Processor maintains an Information Security Management System (ISMS) certified in accordance with ISO/IEC 27001:2022. Within this framework, the Processor implements technical and organisational measures designed to ensure a level of security appropriate to the risks associated with the processing of Personal Data in accordance with Article 32 GDPR.

These measures include structured information security governance and risk management processes, identity and access management controls, encryption of data in transit and where appropriate at rest, network and infrastructure protection mechanisms, system monitoring and logging, vulnerability management and regular patching procedures, as well as backup and disaster recovery capabilities. The Processor also maintains physical and organisational safeguards protecting the environments in which Personal Data is processed.

The Processor regularly reviews and improves these safeguards as part of the continuous improvement processes of its certified ISMS.

Sub-processors

The Processor may engage Sub-processors where this is necessary to support the delivery of the Services. In such cases, the Processor shall ensure that Sub-processors are contractually bound to data protection obligations equivalent to those set out in this DPA. The Processor remains responsible for the performance of its Sub-processors and for ensuring that Personal Data processed by such parties remains protected in accordance with applicable data protection laws.

Information regarding Sub-processors used in connection with the Services shall be made available to the Controller through appropriate documentation or through a publicly available list maintained by the Processor. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors through updates to such documentation or list.

If the Controller has reasonable data protection concerns regarding a newly appointed Sub-processor, the Controller may object to the engagement of that Sub-processor within a reasonable period after receiving notice. In such case, the parties shall work in good faith to resolve the concern. If the concern cannot be resolved within a reasonable time, the Controller may terminate the affected Services in accordance with the termination provisions of the Agreement.

Personal Data Breaches

If the Processor becomes aware of a Personal Data breach affecting Personal Data processed under this DPA, the Processor shall notify the Controller without undue delay and, where feasible, within 72 hours after becoming aware of the breach. The Processor shall provide the Controller with information reasonably necessary to enable the Controller to comply with its notification obligations under Articles 33 and 34 GDPR. Such notification shall include, where available, a description of the nature of the breach, the categories of data affected, the likely consequences of the breach, and the measures taken or proposed by the Processor to mitigate or remedy the situation.

Data Subject Rights

Considering the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures to enable the Controller to respond to requests from data subjects exercising their rights under applicable data protection law. These rights may include, among others, the rights of access, rectification, erasure, restriction of processing, data portability and objection to processing.

International Data Transfers

Personal Data shall generally be processed within the European Economic Area. Where it becomes necessary to transfer Personal Data outside the European Economic Area, the Processor shall ensure that such transfers are carried out in accordance with the requirements of applicable data protection law.

Where required under applicable data protection law, the parties agree that the Standard Contractual Clauses adopted by the European Commission pursuant to Article 46 GDPR ("SCCs") shall be deemed incorporated by reference into this DPA and shall apply to such transfers. Where relevant, the SCCs shall be supplemented by the UK International Data Transfer Addendum or the Swiss Federal Data Protection and Information Commissioner supplement, as applicable.

The parties shall implement any additional safeguards reasonably necessary to ensure that such international transfers provide an adequate level of protection for Personal Data in accordance with applicable data protection law.

Return or Deletion of Data

Upon termination or expiration of the Agreement, the Processor shall, at the choice of the Controller, either return all Personal Data to the Controller or securely delete such Personal Data within a reasonable period following termination. The Processor may retain residual copies of Personal Data in secure backup systems for a limited period where such retention is technically unavoidable, provided that such data remains protected in accordance with this DPA and is deleted in accordance with the Processor's standard backup retention cycle. Where the Processor is required to retain certain Personal Data under applicable law, such data may be retained for the duration required by that law and shall remain protected in accordance with this DPA.

Audit and Compliance

The Processor shall make available to the Controller information reasonably necessary to demonstrate compliance with this DPA and applicable data protection law. In particular, the Processor may satisfy this obligation by providing relevant security documentation, evidence of certifications such as ISO/IEC 27001:2022, or summaries of independent third-party audits.

Only where such information is insufficient may the Controller request a further audit. Any such audit shall be subject to reasonable prior notice, be limited to matters directly related to the processing of Personal Data under this DPA and be conducted in a manner that does not unreasonably interfere with the Processor's operations or compromise the security of other customers' systems or data. On-site inspections shall only be permitted where the information and documentation provided remotely are insufficient to demonstrate compliance and shall be subject to appropriate confidentiality and security restrictions designed to protect the Processor's systems, facilities and other customers' information.

Liability

Liability between the parties in connection with the processing of Personal Data shall be governed by the liability provisions set out in the Agreement and applicable data protection law. Nothing in this DPA shall limit or exclude either party's liability towards data subjects under Article 82 GDPR or restrict any mandatory liability arising under applicable data protection law.

Term

This DPA shall remain in effect for as long as the Processor processes Personal Data on behalf of the Controller under the Agreement.

Annex I – Description of Processing

Subject Matter of the Processing. The processing concerns the provision, operation and maintenance of the Innerspace SaaS platform and associated services under the Agreement.

Duration of the Processing. Personal Data is processed for the duration of the Services Agreement between the parties and for any additional period required to complete return or deletion obligations under the DPA, unless retention is required by applicable law.

Nature of the Processing. Processing activities include the hosting, storage, organisation, retrieval and transmission of Personal Data within the platform environment, as well as the maintenance of operational and security logs and the provision of technical support and system maintenance services.

Purpose of the Processing. The purpose of the processing is to enable the delivery and operation of the Services for the Controller, including the delivery of digital training content, the recording and analysis of training progress and performance metrics, system security and integrity monitoring, and customer support.

Categories of Data Subjects. Data subjects may include employees, trainees, contractors, administrators, platform users or other individuals whose Personal Data is submitted to the Services by or on behalf of the Controller.

Categories of Personal Data. Personal Data processed within the Services may include names, email addresses, user identifiers, training progress and performance information, usage or interaction data, device identifiers and system log data.

Annex II – Security Framework

The Processor may update or replace the technical and organisational security measures implemented within its Information Security Management System from time to time, provided that such updates do not materially reduce the overall level of protection for Personal Data.

The Processor operates an Information Security Management System certified according to ISO/IEC 27001:2022. Within this framework, the Processor maintains policies, procedures and technical safeguards designed to protect the confidentiality, integrity and availability of information.

Security controls implemented within this framework are aligned with ISO/IEC 27001 Annex A and cover areas such as access control management, asset management, cryptographic protection, operational security processes, communications security, supplier security management, incident management procedures, as well as business continuity and disaster recovery capabilities.

Further details regarding the security framework may be made available to the Controller through security documentation or relevant audit reports upon reasonable request.

Annex III – List of approved Sub-Processors

Name	VAT	Address
Microsoft Österreich GmbH	ATU15162507	A-1120 Wien Am Euro Platz 3
Microsoft Ireland Operations Limited	IE 825 39822	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18
Amazon Web Services EMEA SARL	ATU7490456	38 Avenue John F. Kennedy, L-1855 Luxembourg
HubSpot Inc.		2 Canal Park Cambridge, MA 02141 United States
Atlassian Pty Ltd	EU372001951	c/o Atlassian 350 Bush St, Floor 13 San Francisco, CA 94104 United States