learningbank

LAST MODIFIED: 04.05.2026

# Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the agreement between the Customer (the "Controller") and Learningbank (the "Processor"), governing the Customer's purchase and use of Learningbank's Products and Professional Services.

It sets out the parties' rights and obligations with respect to the processing of personal data in accordance with applicable data protection laws and remains in effect for the duration of the Agreement.

Capitalised terms not defined in this DPA have the meanings set forth in the Agreement, and we may update this DPA from time to time in accordance with section 5.1.

## Contents


1. Background
2. Definitions
3. Processing of Personal Data
4. Security Measures
5. Sub-processing
6. Transfer of Personal Data to a Third Country
7. Data Processor's General Obligations
8. Liability
9. Termination
10. Jurisdiction and Choice of Law


## Schedules


- Schedule 1: Data Processing Instructions
- Schedule 2: Sub-processors and locations for processing of personal data

## 1. Background

1.1. The Data Controller and Data Processor have entered into an agreement concerning Data Controller's purchase of a learning platform provided by Data Processor (the "**Master Agreement**"). The scope of the learning platform will be training of Data Controller's employees.

1.2. As part of Data Processor's provision of Services (as defined below) to Data Controller under the Master Agreement, Data Processor will be processing personal data on behalf of Data Controller.

1.3. Applicable Data Protection Legislation (as defined below) requires that a written contract be entered into between a data controller and data processor, who processes personal data on behalf of the data controller, governing the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller. Accordingly, the Parties have entered into this Data Processing Agreement (as defined below).

1.4. The Master Agreement and the Data Processing Agreement are interdependent and cannot be terminated separately. The Master Agreement and the Data Processing Agreement are subject to the Terms and Conditions (as defined below).

1.5. In the event of any inconsistency between the contents of the Master Agreement or the Terms and Conditions and the Data Processing Agreement in relation to data protection obligations, the Data Processing Agreement will prevail irrespective of any previous agreements between the Parties.

## 2. Definitions

2.1. Terms defined in the Master Agreement shall have the same meaning when used in this Data Processing Agreement, unless otherwise expressly stated herein.

2.2. In this Data Processing Agreement, unless the context otherwise requires:

- "Master Agreement" has the meaning ascribed to it in clause 1.
- "Data Processing Agreement" means this data processing agreement, including Schedules.
- "Data Protection Legislation" means all the laws and rules governing the processing and protection of personal data throughout the European Economic Area (EEA) as amended, supplemented and/or modified from time to time, including the General Data Protection Regulation (as defined below), relevant national legislation and, where relevant, the guidelines and rules issued by the Danish Data Protection Agency or other competent supervisory authorities in the EEA (including the national supervisory authorities).
- "General Data Protection Regulation" means "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" as amended, supplemented and/or modified from time to time.
- "Services" means the services and supplies provided by Data Processor as provider to Data Controller as customer under the Master Agreement.
- "Terms and Conditions" means general terms and conditions that apply to all of Data Processor' products and services and, where relevant, specific terms and conditions that apply to the individual products only, applicable at any time.
- The terms "personal data", "special categories of personal data", "process/processing", "controller", "processor", "data subject", "supervisory authority", "pseudonymisation", "technical and

organisational measures" and "personal data breach" as used in this Data Processing Agreement shall be understood in accordance with the Data Protection Legislation, including the General Data Protection Regulation.

## 3. Processing of personal data

3.1. Data Processor shall process personal data on behalf of Data Controller in accordance with the Data Protection Legislation.

3.2. The personal data to be processed by Data Processor and the categories of data subjects are set out in schedule 1 to this Data Processing Agreement.

3.3. Data Processor may only process the personal data on documented instructions from Data Controller, unless required to do so pursuant to mandatory European Union rules and regulation or mandatory member state law to which Data Processor is subject. In that case, Data Processor must notify Data Controller of such legal requirement before the processing, unless the relevant law prohibits such notification on important grounds of public interest.

3.4. Data Processor must ensure that the persons involved in the processing of personal data on behalf of Data Controller under the Data Processing Agreement have either committed themselves to confidentiality or are subject to a proper statutory duty of confidentiality and that they only process personal data in compliance with the Master Agreement, the Data Processing Agreement and the Data Protection Legislation.

3.5. Data Processor shall take the necessary steps to ensure that any person acting under the authority of Data Processor, and who has access to the personal data, does not process such personal data except on documented instructions from Data Controller.

3.6. Data Processor shall, upon request from Data Controller, provide access to all necessary information in order for Data Controller to ensure compliance with the obligations laid down in the Data Protection Legislation.

3.7. The Data Processor shall during the term of the Data Processing Agreement and upon request from Data Controller issue an annual audit report on the Data Processor's IT Security and the Data Processor shall bear the costs.

3.8. Furthermore, Data Processor must allow and contribute to any audits, including inspections, conducted by Data Controller or an auditor authorized by Data Controller, which must be bound to confidentiality, selected by the Data Controller and approved by Data Processor, and, where applicable, in coordination with the supervisory authority. Data Processor is entitled to receive separate compensation in this regard.

3.9. The audits carried out by Data Controller or an auditor authorized by Data Controller must be proportional with regard to the sensitivity of the personal data processed by Data Processor.

3.10. Data Processor must immediately notify Data Controller if, in Data Processor's opinion, an instruction from Data Controller is contrary to the Data Protection Legislation.

## 4. Security measures

4.1. Taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of the processing as well as risk of varying likelihood and severity of the rights and freedoms of natural persons, Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

4.2. Data Processor shall assist Data Controller by appropriate technical and organizational measures with the fulfilment of Data Controller's obligation to respond to requests for exercising the data subject's rights as laid down in the Data Protection Legislation.

4.3. Data Processor shall notify Data Controller without undue delay after becoming aware of a personal data breach. Furthermore, Data Processor shall assist Data Controller in ensuring compliance with Data Controller's obligations (i) to document any personal data breach, (ii) to notify the applicable supervisory authority/ies of any personal data breach, and (iii) to communicate such personal data breaches to the applicable data subjects in accordance with Articles 33 and 34 of the General Data Protection Regulation.

## 5. Sub-processing

5.1. By signing this Data Processing Agreement, Data Controller agrees that Data Processor may engage Sub-Contractors to assist in providing the Services. The list of sub-contractors currently engaged in processing personal data (hereinafter referred to as Sub-Processors) and the countries and facilities in which the personal data is processed, is enclosed as schedule 2 to this Data Processing Agreement.

Any additions and/or changes to the list will be notified to Data Controller via email. Notification shall be given no less than thirty (30) calendar days before the contemplated sub-processing is put into effect. If Data Controller wishes to object to the sub-processing, Data Controller shall state so in writing within fourteen (14) calendar days of receiving the before mentioned notification. Data Controller's objection must be specific and justifiable. Absence of any objections from Data Controller shall be considered as a consent to the sub-processing.

5.2. Data Processor shall ensure that the sub-processing is lawful and that any and all Sub-Processors undertake and are subject to the same terms and obligations as Data Processor as set out herein.

5.3. Data Processor warrants the legality of its Sub-Processors' processing of personal data. Data Processor shall remain responsible for all acts and omissions of its Sub-Processors, and the acts and omissions of those employed or engaged by Sub-Processors, as if such acts and omissions were performed by Data Processor itself.

## 6. Transfers of personal data to a third country

6.1. The Processor may transfer personal data to countries outside the EU/EEA where necessary for the provision of the services.

6.2. The Processor will ensure that any such transfers are carried out in accordance with applicable data protection laws, including Chapter V of the GDPR (Articles 44–49), and that appropriate safeguards are in place, including, where applicable, the European Commission's Standard Contractual Clauses.

6.3. Sub-processors are listed in Annex II.

## 7. Data processor's general obligations

7.1. Data Processor shall apply and comply with the Data Protection Legislation and shall not perform its obligations under the Master Agreement and the Data Processing Agreement in such a way as to cause Data Controller to breach any of its obligations under applicable Data Protection Legislation.

7.2. Data Processor must assist Data Controller in ensuring compliance with any of Data Controller's obligations pursuant to the Data Protection Legislation, including for instance obligations pursuant to Article 35 (Data protection impact assessment) and Article 36 (Prior consultation) of the General Data Protection Regulation. Data Processor is entitled to receive separate compensation regarding such assistance and the specific compensation will be agreed upon separately.

## 8. Liability

8.1. Data Processor shall only be liable for the damage caused by processing of personal data where Data Processor has not complied with obligations of the Data Protection Legislation that are specifically directed to data processors or where Data Processor has acted outside or contrary to lawful instructions of Data Controller. Data Processor's total liability towards Data Controller arising from breach of this Data Processing Agreement cannot exceed more than the total amount paid the Data Controller to Data Processor under the Agreement for the last twelve (12) months.

## 9. Termination

9.1. This Data Processing Agreement shall automatically terminate upon any termination or expiration of the Master Agreement.

9.2. The Parties agree that at the termination or expiry of the Master Agreement and/or the Data Processing Agreement, (i) Data Processor permits Data Controller to export the personal data under this DPA in accordance with the capabilities of the Platform. (ii) Upon day of expiry Data Processor will delete all data processed under the Master Agreement and the Data Processing Agreement and certify to Data Controller that this has been done, including for avoidance of doubt delete such data from any computer, server, and/or any other storage device or media, unless European Union and/or member state law requires storage of such personal data.

9.3. Notwithstanding clause 9.1 Data Processor will retain all personal data processed under this Data Processing Agreement for 30 days after the termination of the Master Agreement. This “retention” will ensure that Data Controller's access to the personal data can be re-established after any conceivable targeted attack against the Data Controller's primary data and backup data. After expiration of the 30 days retention period, Data Processor will delete all records of Data Controller's personal data without undue delay.

## 10. Jurisdiction and choice of law

10.1. This Data Processing Agreement shall be governed by Danish law. Any disputes arising out of or in connection with the provisions of this Data Processing Agreement shall be settled by the Copenhagen City Court as the agreed venue.

# Annex I
# Data Processing Instructions

## 1. Purposes

A. Provisioning of personnel administrative, as to deliver a learning platform (SaaS), used to plan, implement, and assess specific learning process in the Data Controller's organisation.

B. In accordance with a) above, the personal data will for instance be subject to the following processing purposes: collection, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

C. Support of the customer, product development and testing to ensure the quality of the product provided in accordance with a) above.

## 2. Categories of data

Ordinary categories of personal data, including but not limited to, name, email address and telephone number, and any other categories of data submitted by Data Controller to Data Processor from time to time for purposes of the Services.

The Data Controller may additionally configure, map, and upload other categories of personal data within the scope of the Services, including via integrations with third-party systems, as determined by the Data Controller.

To the extent the Data Controller integrates the Services with third-party systems or uploads personal data via integrations, the Data Controller is responsible for determining the categories of personal data transferred and ensuring that such transfers are lawful.

The Data Processor processes such personal data solely in accordance with the Data Controller's instructions as implemented through the Services and does not independently verify the lawfulness or accuracy of such data.

## 3. Categories of Data Subjects

Data Controller's employees (specific: B2B Customers and their employees).

## 4. Processing Operations

The personal data will for instance be subject to the following processing operations: collection, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission to sub-processors, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

## 5. Location of Processing Operations:

Processing operations are in the EU with hosting in Dublin and Frankfurt through AWS.

## 6. Information Security

Processing by Data Processor will be subject to the following security measures:

- Data Processor must ensure that the employees of Data Processor engaged in the processing of personal data are bound by a duty of confidentiality. Only employees authorised to access Data Controller's personal data may access such data.
- Data Processor must ensure that the employees of Data Processor receive adequate training in and instructions on data protection.
- Data Processor must impose adequate restrictions on physical access.
- Data Processor must ensure that access to personal data is restricted to employees and, if relevant, to suppliers having a work-related need for access. Access rights will be subject to prior approval from Data Processor and must be withdrawn immediately once the individual in question no longer satisfies the criteria for such access.
- Access rights will be subject to regular review.
- Data Processor must apply suitable authentication mechanisms such as access codes, etc., and such mechanisms must as a minimum satisfy the requirements considered to be adequate/prudent within the relevant area. This applies e.g. to the length and composition of passwords.
- Data Processor must apply adequate technical measures to limit the risk of unauthorised access and abuse of personal data. Such measures must basically include firewall, anti-virus software, and malware protection. Data Processor must implement formal procedures to ensure that the security systems are updated.
- Data Processor must use encryption or similar measures to the extent required by the Data Protection Legislation.
- Data processor must carry out any tests in a separate environment.
- Data Processor must implement procedures for the handling of security breaches.
- Data Processor must ensure that personal data are erased before equipment is disposed of or passed on to a third party.

# Annex II – Sub-processor(s)

The Processor uses the following sub-processors in connection with the provision of the services:

| Sub-processor | Location | Processing activity | Purpose |
|---|---|---|---|
| Amazon Web Services, Inc. | EU (Ireland) | IT infrastructure, hosting and backups | Cloud hosting provider for Learningbank's services, including back-up storage |
| Linear Orbit, Inc. | EU (Belgium) | Support and issue tracking | Used internally for handling complex support requests requiring involvement from the development team |
| HubSpot, Inc. | EU (Ireland) | Customer relationship management | CRM tool used for managing customer contacts and communication |
| Kombo Technologies GmbH | EU (Germany) | Integrations | Integration platform used to enable customer-managed integrations with third-party systems |
| Celonis (Make.com) | EU (Germany) | Integrations | Platform used to enable customer-managed custom integrations |
| Intercom R&D Unlimited Company | EU (Ireland) | Support | Through Data Processor's integrated support system, platform administrators can access email and chat support, as well as the Help Center. For requests related to service functionality, these are connected to Linear. |