

Note to copy: The Learningbank Data Processing Agreement is made available at learningbank.io/dpa and is incorporated into the Learningbank Customer Terms of conditions signed with your Master Agreement.

For Customers that would like to receive a signed copy of the Learningbank Data Processing Agreement, we have made this copy available to you. This copy includes signatures on the Data Processing Agreement version last modified January 11, 2021. No changes made to this copy are agreed to by Learningbank, or its affiliates. Please note that we update the Data Processing Agreement as we describe in the section below. Current Data Processing Agreement terms are available at learningbank.io/dpa, and from today's date be archived Data Processing Agreement terms that are available at learningbank.io/dpa-archive. If you have any questions, please contact compliance@learningbank.io

DATA PROCESSING AGREEMENT

LAST MODIFIED: 11.01.2021

PARTIES

This Data Processing Agreement ("DPA") forms part of the Master Agreement entered into by Data Controller and Data Processor hereinafter collectively referred to as "**Parties**" and separately as a "**Party**", pursuant to which the Data Controller has purchased Learningbanks services.

The purpose of this DPA is to reflect the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Applicable Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Master Agreement, as applicable.

We update these terms from time to time and we follow the procedures as described in section 5.1. The term of this DPA will follow the term of the Master Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

COTENTS

1.	BACKGROUND	4
2.	DEFINITIONS	4
3.	PROCESSING OF PERSONAL DATA	5
4.	SECURITY MEASURES	5
5.	SUB-PROCESSING	6
6.	TRANSFERS OF PERSONAL DATA TO A THIRD COUNTRY	6
7.	DATA PROCESSOR'S GENERAL OBLIGATIONS	6
8.	LIABILITY	7
9.	TERMINATION	7
10.	JURISDICTION AND CHOICE OF LAW	7

SCHEDULES

Schedule 1	Categories of data subjects, types of personal data and processing activities [as well as security measures]
Schedule 2	List of sub-processors and location(s) 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:
 1. "**Master Agreement**" has the meaning ascribed to it in clause 1.1.
 2. "**Data Processing Agreement**" means this data processing agreement, including Schedules.
 3. "**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).
 4. "**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.
 5. "**Services**" means the services and supplies provided by Data Processor as provider to Data Controller as customer under the Master Agreement.
 6. "**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.

2.3 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 fourteen (14) 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 seven (7) 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

By signing this Data Processing Agreement, Data Controller accepts that Data Processor may transfer personal data to a third country, i.e. a country outside the EEA. Data Processor will be required to ensure that such transfer is at all times lawful, including i.e. that there is an adequate level of protection of the transfer of the personal data. Please also see Schedule 2, personal data is only transferred to a third country in connection with support, not as part of the normal processing.

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, Data Processor shall, at the choice of Data Controller, (i) return all data processed under the Master Agreement and/or the data Processing Agreement and any copies thereof to Data Controller, or (ii) 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 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

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.

11. SIGNATURES

EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES:

FOR DATA PROCESSOR

FOR DATA CONTROLLER

Katrine Schelbli

Signature
Name: Katrine Schelbli
Position: COO – Chief Operating Officer

Signature
Date
Name:
Position:

Annex I – CATEGORIES OF DATA SUBJECTS, TYPES OF PERSONAL DATA AND PROCESSING ACTIVITIES AS WELL AS SECURITY MEASURES CARRIED OUT BY DATA PROCESSOR

This Schedule forms an integral part of the Data Processing Agreement and must be filled in by the Parties.

1. CATEGORY OF DATA SUBJECTS AND TYPES OF PERSONAL DATA

Schematic overview of categories of data subjects and types of personal data processed		
Category of data subjects: Data Controller's employees	<input checked="" type="checkbox"/> Ordinary categories of personal data, including but not limited to, name, email address and telephone number.	
	Special categories of personal data (tick box):	
	<input type="checkbox"/> Racial origin <input type="checkbox"/> Ethnic origin <input type="checkbox"/> Political opinions <input type="checkbox"/> Religious belief <input type="checkbox"/> Philosophical belief <input type="checkbox"/> Trade union membership	<input type="checkbox"/> Genetic data <input type="checkbox"/> Biometric data for the purpose of uniquely identifying natural person <input type="checkbox"/> Data concerning health <input type="checkbox"/> Data concerning sex life <input type="checkbox"/> Data concerning sexual orientation
	<input type="checkbox"/> CPR (civil registration number)	<input type="checkbox"/> Personal data relating to criminal convictions and offence

2. PROCESSING ACTIVITIES

The definition of processing in the General Data Protection Regulation:

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The personal data will for instance be subject to the following processing activities:

collection, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. SECURITY MEASURES

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.
- Any tests must be carried out 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 – LIST OF SUB-PROCESSORS AND LOCATION(S) FOR PROCESSING OF PERSONAL DATA

This Schedule forms an integral part of the Data Processing Agreement and must be filled in by the Parties.

1. SUB-PROCESSOR(S)

Data Processor is entitled to use the following Sub-Processors:

Name	Address	Specifications of the processing of personal data	The processing of data takes place on the following location(s)
Amazon Web Services, Inc.	410 Terry Ave North Seattle, WA	IT infrastructure incl. storage	<p>The processing of data takes place on the following location: EU (Ireland)</p> <p>Amazon Web Services certification: ISO 27001, ISO 27017 and ISO 27018.</p> <p>The AWS GDPR Data Processing Addendum with Standard Contractual Clauses (SCC) is part of the AWS Service Terms.</p> <p>Amazon Web Services does not access or use your content for any purpose. Data is only stored in Ireland, and not in the US. Amazon will not move or replicate your content outside EU (Ireland).</p>
Atlassian Pty Ltd.	Level 6 341 George Street Sydney, NSW 2000 Australia	Support process, only ad hoc.	<p>The processing of data takes place on the following location: US/EU/AU</p> <p>Atlassian certification: ISO 27001 and ISO 27018.</p> <p>Data Transfers from Europe to the US, Atlassian adheres to Standard Contractual Clauses (SCC) to transfer data from the EEA and UK to the US. Although Privacy Shield has been invalidated, Atlassian is still committed to honouring its obligation regarding data protection under its framework. Atlassian follows the EU GDPR-rules.</p> <p>The product that we use from Atlassian does not process any other data than what you feed it with. Any upload to Atlassian is handled manually by a Learningbank employee from our customer support.</p>
Microsoft – Office365	1 Microsoft Way, Redmond, WA 98052	Support process, only ad hoc.	<p>The processing of data takes place on the following location: EU (Netherlands/Ireland)</p> <p>Microsoft certification: ISO 27001.</p>

			<p>Data Transfers from Europe to the US, Microsoft adhere to Standard Contractual Clauses (SCC). Although Privacy Shield has been invalidated, Microsoft has been using both SCC and Privacy Shield for several years.</p> <p>Microsoft does not process any other data than what you feed it with.</p>
Salesforce.com Inc.	San Francisco (HQ), CA United States 415 Mission St 3rd Floor	Customer relationship management (CRM), only ad hoc.	<p>The processing of data takes place on the following location: EU (Germany/France)</p> <p>Salesforce certification: ISO 27001, ISO 27017 and ISO 27018.</p> <p>Salesforce's services pursuant to Salesforce's Processor Binding Corporate Rules (BCR) and the Standard Contractual Clauses (SCC), both of which are incorporated by reference into Salesforce's Data Processing Addendum.</p> <p>Any upload to Salesforce is handled manually by a Learningbank employee from our customer support.</p>
Zendesk Inc.	1019 Market St., San Francisco, CA 94103	Support process, only ad hoc.	<p>The processing of data takes place on the following location: US</p> <p>Zendesk certification: ISO 27001 and ISO 27018.</p> <p>Zendesk has obtained regulatory authorization of its controller and processor Binding Corporate Rules (BCR) for its customers' data, which provide a robust mechanism to transfer personal data from the EU to members of the Zendesk family of companies when using our services.</p> <p>Zendesk does not process any other data than what you feed it with.</p>
Wrike, Inc.	10 Almaden Blvd. Ste 1000, San Jose, CA 95113	Project Management,	<p>The processing of data takes place on the following location: EU (Netherlands)</p> <p>Wrike's services pursuant to the European Commission's Standard Contractual Clauses (SCC), both of which are incorporated by reference into Wrike's Data Processing Addendum.</p> <p>Wrike certification: ISO 27001, a and compliant with</p>

			<p>ISAE 3492.</p> <p>Any upload to Wrike is handled manually by a Learningbank employee based on customer request.</p>
Blendr NV	<p>Grauwpoort 1, 9000 Ghent, Belgium</p>	Integrations	<p>The processing of data takes place on the following location: EU (Belgium)</p> <p>Blendr certification: ISO 27001</p> <p>Blendr meets all internal standards in information security. Blendr does not access or use your content for any purpose. Data is only accessible in Belgium, and not in the US. Blendr will not move or replicate your content outside Belgium.</p>
Intercom	<p>San Francisco (HQ), CA United States</p> <p>KPMG Building, 55 2nd St 4th floor, San Francisco</p>	Support process, only ad hoc.	<p>The processing of data takes place on the following location: EU (Ireland)</p> <p>Encryption: AES-256</p> <p>Data is only handled in EU (Ireland), and when we refer to Intercom, we mean Intercom R&D Unlimited Company, a company registered in Ireland. Intercom relies on Standard Contractual Clauses (SCC).</p> <p>Intercom does not process any other data than the one you feed it with.</p>
Productboard	<p>San Francisco (HQ), CA United States</p> <p>612 Howard St, San Francisco</p>	Support process, only ad hoc.	<p>The processing of data takes place on the following location: US</p> <p>Productboard certification: ISO 27001</p> <p>Productboard complies with the GDPR and EU Data Protection laws in general. To allow transfers of personal data from EU member counties; the Standard Contractual Clause (SSC) have been incorporated.</p>
Hubspot	<p>25 First Street, 2nd Floor, Cambridge, MA 02141, United States.</p>	Only ad hoc.	<p>The processing of data takes place on the following location: US</p> <p>Hubspot certification: ISO 27001</p> <p>Hubspot complies with the GDPR and EU Data Protection laws in general. To allow transfers of personal data from EU member counties; the Standard Contractual Clause (SSC) have been incorporated.</p>

--	--	--	--

On behalf of the data exporter

FOR DATA PROCESSOR

Katrine Schelbli

Signature

Name: Katrine Schelbli

Position: COO – Chief Operating Officer

FOR DATA CONTROLLER

Signature

Name:


Position:

Date

Signature Certificate

Document Ref.: 8RVPH-PPGQG-GGF6T-MRUAC

Document signed by:

	<p>katrine Schelbli Verified E-mail: ks@learningbank.io</p>	<p><i>Katrine Schelbli</i></p> 
<p>IP: 152.115.185.18</p>		<p>Date: 13 Jan 2021 10:03:22 UTC</p>

Document completed by all parties on:
13 Jan 2021 10:03:22 UTC

Page 1 of 1



Signed with PandaDoc.com

PandaDoc is the document platform that boosts your company's revenue by accelerating the way it transacts.

