

## **Data Processing Agreement for Educational Institutions (Annex to the License Agreement)**

### **1. Preamble**

The Client (“**Controller**”) has commissioned Ableton (“**Data Processor**”) in the License Agreement (hereinafter referred to as the “**Main Agreement**”) for the services specified therein. Part of the execution of the Main Agreement is the processing of personal data. Art. 28 GDPR imposes specific requirements on such commissioned processing. To comply with these requirements, the Parties enter into the following Data Processing Agreement (hereinafter referred to as the “**DPA**”) as integral part of the Main Agreement, the performance of which shall not be remunerated separately unless expressly agreed.

### **2. Subject of the DPA**

The Data Processor provides the services specified in the Main Agreement for Controller, in particular by providing software (“**Software**”). In doing so, Data Processor obtains access to personal data, which Data Processor processes for Controller exclusively on behalf of and in accordance with Controller's instructions. The scope and purpose of the data processing by the Data Processor are set out in the Main Agreement; Data Processor will process personal data while fulfilling the Main Agreement vis-à-vis Controller.

The Parties conclude this DPA to specify the mutual rights and obligations under data protection law. The terms of this DPA apply in addition to the terms of the Main Agreement; in case of contradictions, the provisions of this DPA shall take precedence over the provisions of the Main Agreement.

The provisions of this DPA shall apply to all activities related to the Main Agreement in which Data Processor and its employees or persons authorized by Data Processor encounter personal data originating from Controller or collected for Controller.

The term of this DPA shall be governed by the term of the Main Agreement unless the following provisions give rise to further obligations or termination rights.

Any term defined the GDPR shall have the same meaning relating to this DPA.

### **3. Right of instruction**

Data Processor may only collect, process or use data within the scope of the Main Agreement and in accordance with the instructions of Controller; this applies in particular to the transfer of personal data to a third country or to an international organization. If Data Processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it shall notify Controller of these legal requirements prior to the processing.

The instructions of Controller shall initially be determined by this DPA. Thereafter, they may be amended, supplemented, or replaced by Controller in writing or text form by individual instructions or by using features of the Software. Controller shall be entitled to issue such instructions at any time. This includes instructions regarding the correction, deletion, and blocking of data. All instructions issued shall be documented by Controller. Instructions that go beyond the service agreed in the Main Agreement shall be treated as a request for a change in service.

If Data Processor is of the opinion that an instruction of Controller violates data protection provisions, it shall notify Controller thereof without undue delay. Data Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by Controller. Data Processor may refuse to carry out an obviously unlawful instruction.

### **4. Location of Data Processing**

Unless explicitly agreed otherwise (e.g. in Appendix 4), the data processing shall take place within the European Union.

### **5. Types of data processed and categories of Data Subjects**

Within the scope of the implementation of the Main Agreement, Data Processor shall have access to the personal data specified in more detail in Appendix 1.

The groups of data subjects affected by the data processing is listed in Appendix 2.

### **6. Protective measures of the Data Processor**

Data Processor shall be obliged to observe the statutory provisions on data protection and not to disclose information obtained from Controller's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons (including against legal attachment or seizure), considering the state of the art.

Data Processor shall organize the internal organization within its field of responsibility in such a way that it meets the special requirements of data protection. It shall have taken the technical and organizational measures specified in Appendix 3 to adequately protect Controller's data pursuant to Art. 32 GDPR, which Controller acknowledges as adequate. Data Processor reserves the right to reasonably adapt the security measures taken while ensuring that the contractually agreed level of protection is not undercut.

The persons employed in the data processing by Data Processor are prohibited from collecting, processing or using personal data without authorization. Data Processor shall oblige all persons entrusted by it with the processing and performance of this

Agreement accordingly (obligation of confidentiality, Art. 28 lit. b GDPR) and shall ensure compliance with this obligation with due care.

Upon request by Controller, the Parties will exchange contact of responsible persons to clarify any professional, technical and organisational issues that may arise.

Data Processor has appointed a data protection officer. Data Processor's data protection officer is Nikolaus Bertermann, daspro GmbH, Kranzler Eck, Kurfürstendamm 21, 10719 Berlin, post@daspro.de)

## **7. Information obligations of the Data Processor**

In the event of disruptions, suspected data protection violations or breaches of contractual obligations of Data Processor, suspected security-related incidents or other irregularities in the data processing by persons employed by it within the scope of the Main Agreement or by third parties, Data Processor shall inform Controller without undue delay. The same shall apply to audits of Data Processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

- a description of the nature of the personal data breach, including, to the extent possible, the categories and the number of data subjects affected, the categories affected and the number of personal data records affected;
- a description of the measures taken or proposed by Data Processor to address the breach and, where applicable; measures to mitigate its possible adverse effects; and
- a description of the likely consequences of the personal data breach.

Data Processor shall immediately take the necessary measures to secure the data and to mitigate any possible adverse consequences for the data subjects, inform Controller thereof and request further instructions.

In addition, Data Processor shall be obliged to provide Controller with information at any time insofar as Controller's data are affected by a breach pursuant to paragraph 1.

## **8. Control rights of Controller**

Controller may satisfy itself of the technical and organizational measures of Data Processor prior to the commencement of data processing and thereafter. For this purpose, Controller may, for example, obtain information from Data Processor, obtain existing certificates from experts, certifications or internal audits or, after timely coordination, personally inspect the technical and organizational measures of Data Processor during normal business hours or have them inspected by a competent third party, provided that the third party is not in a competitive relationship with Data Processor. Controller shall carry out checks only to the extent necessary and shall not disproportionately disrupt the operations of Data Processor in the process. In case of on-site inspection, Controller will reimburse Data Processor for any related costs within an appropriate scope including the personnel costs generated through the guidance and support of any controlling persons on-site.

Data Processor undertakes to provide Controller, upon request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures of Data Processor.

Controller shall document the results of the inspection and notify Data Processor thereof. In the event of errors or irregularities which Controller discovers, in particular during the inspection of the results of the inspection, Controller shall inform Data Processor without undue delay. If issues are, Controller shall notify Data Processor of the necessary procedural changes without delay.

In case that a government supervisory agency undertakes measures against Controller in accordance with Art. 58 GDPR – particularly with regards to notification and controlling obligations, Data Processor will issue any required information to Controller and will enable the responsible government supervisory agency to conduct on-site controlling measures. Controller must be notified by the Data Processor of the planned measures.

## **9. Use of Sub-Processors**

Data processing relating to the contractually agreed services shall be performed with the involvement of the service providers named in Appendix 4 (hereinafter "Sub-processors"). Controller grants Data Processor its general authorization within the meaning of Article 28 s. 1 GDPR to engage additional Sub-processors within the scope of obligations under the Main Agreement or to replace Sub-processors already engaged.

Data Processor shall inform Controller in advance of any intended change regarding the involvement or replacement of a Sub-processor. Controller may object to an intended enlistment or substitution of a Sub-processor for good cause under data protection law.

The objection to the intended involvement or replacement of a Sub-processor must be raised within two (2) weeks of the information to Controller. If no objection is raised, the involvement or replacement shall be deemed approved. If there is good cause under data protection law and a mutually agreeable solution cannot be found between Controller and Data Processor, Controller shall have a special right of termination at the end of the month following the objection.

When engaging Sub-processors, Data Processor shall oblige them in accordance with the provisions of this DPA.

A Sub-processor relationship within the meaning of these provisions does not exist if Data Processor commissions third parties with services that are purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by Data Processor to Controller and guarding services.

## 10. Requests and rights of Data Subjects

Data Processor shall support Controller with suitable technical and organizational measures in fulfilling Controller's obligations pursuant to Articles 12 to 22 and 32 to 36 GDPR.

If a data subject asserts rights, such as the right of access, correction or deletion regarding his or her data, directly against Data Processor, the latter shall not react independently but shall refer the data subject to Controller and await Controller' instructions.

In case of data subject requests, Controller will reimburse Data Processor for any related costs within an appropriate scope.

## 11. Termination of Main Agreement

After termination of the Main Agreement, Data Processor shall return to Controller all documents and data provided or - at the request of Controller, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This shall also apply to any data backups at Data Processor. Data Processor shall on request provide documented proof of the proper deletion of any data.

Controller shall have the right to control the complete and contractual return or deletion of the data at Data Processor in an appropriate manner.

Data Processor shall be obligated to keep confidential the data of which it has become aware in connection with the Main Agreement even beyond the end of the Main Agreement. This DPA shall remain valid beyond the end of the Main Agreement as long as the Data Processor has personal data at its disposal which have been forwarded to it by the Controller or which it has collected for the Controller.

## Appendix

### Appendix 1 - Description of the data/data categories

Names, e-mail addresses, IP addresses, usage data relating to Data Processor's products

### Appendix 2 - Description of affected Data Subjects

Students of Controller (being an educational organization), employees of Controller (e.g. teachers and IT admins)

### Appendix 3 - Technical and organizational measures of the Data Processor

#### 1. General

The hosting of the data described in this DPA takes place on Data Processor's servers which are located here:

NorthC Datacenters, Gradestraße 60, 12347 Berlin, Germany

(Relevant certifications of datacenters: e.g. ISO/IEC 27001, ISO 22301, ISAE 3402 Type II)

(Additional processing by subprocessors is described in Appendix 4)

#### 2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

##### 2.1 Physical access control

The following implemented measures prevent unauthorized persons from gaining access to the data processing facilities:

Datacenter:

- Remote 24/7 security monitoring
- Full electronic access control system, based on proximity cards with photo and PIN keypads with 2-factor authentication
- Locks on colocation suites and cabinets.
- Intruder detection system on escape and riser doors
- CCTV monitoring and recording of all access points and circulation areas

Offices:

- Access to Ableton's premises is restricted using access tokens, door locks, etc.
- Alarm systems

## 2.2 System access control

The following implemented measures prevent unauthorized persons from accessing the systems of Data Processors:

- Authentication with user and password regarding personal with access to user data
- Management of user permissions
- Use of 2-factor authentication

## 2.3 Data access control

The following implemented measures ensure that unauthorized persons do not have access to personal data in Data Processor's systems:

- Number of administrators is kept as small as possible
- Management of user rights by system administrators

## 2.4 Separation control

The following measures ensure that personal data collected for different purposes are processed separately:

- Separation of production and test systems
- Encryption of data sets processed for the same purpose in database

## 3. Integrity (Art. 32 para. 1 lit. b GDPR)

### 3.1 Transfer control

Means like encryption are used to that personal data cannot be read, copied, modified or removed without authorization during transmission or storage on data carriers.

### 3.2 Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Manual or automatic control of the logs
- Traceability of the input, modification and deletion of data through individual usernames (not user groups)

## 4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Regular backups
- Control of the backup process
- Storage of data backups in a secure, off-site location
- Regular data recovery testing and logging of results
- Separation of operating systems and data

## 5. Procedures for regular review, assessment and evaluation (Art. 32 (d) GDPR; Art. 25 GDPR)

### 5.1 Data Protection Management

The following measures are intended to ensure that an organization that meets the basic requirements of data protection law is in place:

- Appointment of the data protection officer (Nikolaus Bertermann, daspro GmbH, Kranzler Eck, Kurfürstendamm 21, 10719 Berlin, post@daspro.de)
- Obligation of employees to maintain data secrecy
- Regular training of employees in data protection
- Keeping an overview of processing activities (Art. 30 GDPR)
- Conducting data protection impact assessments, if required (Art. 35 GDPR).

## 5.2 Incident Response Management

The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches:

- Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR).
- Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR vis-à-vis the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches

## 5.3 Data protection-friendly default settings (Art. 25 GDPR)

The following implemented measures consider the requirements of the "Privacy by design" and "Privacy by default" principles:

- Training of employees:
- No more personal data is collected than is necessary for the respective purpose.

## 5.4 Order control

The following measures ensure that personal data can only be processed in accordance with instructions:

- Written instructions to the Sub-Processors or instructions in text form (e.g. in the respective data processing agreement or use of respective software frontend).
- Confirmation from Sub-Processors that they commit their own employees to data secrecy (in the respective data processing agreement)

## Appendix 4 – Sub-Processors

Name	Function	Server location
Emarsys eMarketing Systems GmbH, Schleissheimer Strasse 80, 85748, Garching bei München-Hochbrück, Germany	e-mailing / newsletters	European Union
Zendesk Inc., 181 Fremont St.; San Francisco, CA 94105, USA	Customer Support Software	USA (Transfer Mechanisms: Zendesk Binding Corporate Rules, EU-US Data Privacy Framework, EU Standard Contractual Clauses)
Salesforce, Inc.; Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA	Storing of User Master Data	USA (Transfer Mechanisms: EU-US Data Privacy Framework, EU Standard Contractual Clauses)