DATA PROCESSING AGREEMENT

EDUDATA.IO

This Data Processing Agreement (DPA) is for EDUDATA (‘Service’), which is run and provided by Cloudpoint Oy and is supplemental to, and forms an integral part of the main agreement, including, the Terms of Service (‘ToS’) and is effective upon its acceptance. In case of any conflict or inconsistency with the terms of the entirety of the Agreements, this DPA will take precedence to the extent of such conflict or inconsistency.

Contracting parties

Cloudpoint Oy (2325703-6), Kuortaneenkatu 2, 00510 Helsinki, Finland (‘Processor’)

and

Customer (‘Controller’)

Table of contents

1. Definitions

Data Controller

- Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (“Controller”)

Data Processor

- Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (“Processors”)

GDPR

- General Data Data Protection Regulation EU 2016/679

Personal data

- Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

  Any other terms not defined in this DPA shall have the same meaning as in the GDPR.

2. Background and Purpose

The Controller has selected the service provider (Cloudpoint Oy) to act as a Processor in accordance with Article 28(3) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, “GDPR”).

This DPA forms an integral part of the Main Agreement concluded between the Parties under which the Processor shall provide the Controller with the Edudata service, which consists of Edudata Compliance, Edudata Compliance Service,

Edudata Privacy and Edudata Security, unless otherwise agreed in the Main Agreement.

The Processor will process information relating to an identified or identifiable natural person on behalf of the Controller.

The detailed data processing practices are described in the Annex 1 of this DPA.

The purpose of this DPA is to agree on the rights and obligations of the Parties involved in the processing activities as required by the GDPR and to safeguard the freedoms and rights of the data subject during processing.

3. Roles and responsibilities

The Processor shall process personal data in accordance with this DPA and the documented instructions of the Controller. Processor shall not use personal data for any purpose other than agreed in this DPA and in the instruction of the Controller. The instructions of the Controller must be compliant with the applicable data protection laws and consistent with this DPA.

If the Processor notices that any instruction given by the Controller is not compliant with the applicable laws or if they are insufficient, the Processor shall inform the Controller of such non-compliance.

The Controller is responsible for having a legal basis for the processing of personal data, for informing the data subjects of the processing of their personal data and for other data controller obligations set out in the GDPR.

The Controller is responsible for informing the Processor of the contact details of their Data Protection Officer and to ensure the contact details are up to date. Contact details are required in order for the Processor to comply with the notification obligations in case of a data breach incident.

4. Technical and organizational measures

The Processor shall maintain appropriate technical and organizational security measures to protect against unauthorized or unlawful processing or access and against accidental loss, destruction or damage. When choosing the security measures, the Processor must take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons.

Detailed description of the employed measures are stipulated in the Annex 2 of this DPA.

5. Obligation to assist

The Processor processes personal data in accordance with this DPA and the instructions from the Data Controller and in compliance with the data protection legislation.

The Processor must take the necessary measures to protect personal data from processing practices that are not in line with the terms of this DPA, the instructions or data protection legislation.

The Processor undertakes to ensure that those working for the Processor comply with the terms of this DPA and are informed of the relevant legislation.

The Processor supports the Controller in ensuring the fulfillment of the obligations laid down in Articles 32-36 of the GDPR, when requested by the Controller.

The Processor undertakes, without undue delay, to inform the Controller of all requests of the data subjects concerning the exercise of the data subject's rights under the GDPR.

The Processor undertakes to support the Controller with appropriate technical and organizational measures so that the Controller is able to respond to requests regarding the exercise of the data subject's rights.

If the support requested from the Processor requires measures that are likely to cause additional costs for the Processor, the Controller will pay the processor a reasonable compensation for providing the support.

6. International transfers

We process personal data on servers located in the European Economic Area (EEA). As a rule, there are no regular transfers of personal data beyond the EEA.

The Controller accepts that in order to provide the Service, the Processor may have Personal Data processed by, and accessible to, its subprocessors outside the Controller's country of domicile.

In case Personal Data is transferred to a country outside the EEA to a subprocessor, or otherwise transferred to, any country outside the EEA that is not recognised by the European Commission as providing an adequate level of protection for personal data, the Processor provides for appropriate safeguards (GDPR V) for example by standard contractual clauses, adopted approved by the European Commission and applicable to the processing by the non-EEA subprocessor, or by any other appropriate safeguard as foreseen in the Regulation.

The storage location and international transfers outside of the EEA are specified in Annex 1.

7. Duty of Confidentiality

The Processor and all natural persons working for the Processor shall observe both confidentiality and professional secrecy during the Processing. The Processor ensures that all natural persons working for the Processor are bound by confidentiality agreement.

The Processor ensures that there is a non-disclosure agreement with the subprocessors and confidentiality agreement in place between the subprocessor and all natural persons working for the subprocessor participating in the processing.

8. Right to audit

The Controller shall have the right to reasonably audit the facilities and processing activities of the Processor to examine the level of protection and security provided for under this DPA, and to assess the Processor's compliance with the provisions of this DPA.

The Controller shall bear all costs for undertaking an audit. The Controller shall inform the Processor at least 30 working days in advance before conducting the audit.

Where an audit may lead to the disclosure of business or trade secrets of the Processor, or threaten the intellectual property rights of the Processor, an independent expert must be employed to carry out the audit, and such expert shall agree to be bound by a confidentiality agreement.

9. Subprocessors

The Processor shall have the right to involve subprocessors to process personal data in connection with the provision of the Service, to the extent such appointment does not lead to non-compliance with the Processor's obligations under this DPA.

The Processor ensures that the involved subprocessors will operate under a data processing agreement with the Processor and comply with data processing obligations substantially similar to the ones contained herein.

The Processor has the right to change its subprocessors. The Processor shall provide the Controller with a prior notice concerning subprocessor changes. In case the Controller objects to the change or to the addition of subprocessors, the Controller shall have the right to terminate the Service.

10. Breaches

The Processor shall, without undue delay after having become aware of it, inform the Controller in writing about any data breaches relating to the personal data, and any other events where the security of personal data processed on behalf of the Controller has been compromised. The Processor's notification about the breach to the Controller shall include at least the following:

- description of the nature of the breach;
- name and contact details of the Processor's contact point;
- description of the measures taken by the Processor to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. Deletion of personal data

Within a reasonable time, but no more than 180 days, after the termination or expiry of this DPA, and after the Controller has permanently ceased to use the Service, the Processor shall return or permanently delete all personal data from the Processor's storage, unless specifically instructed otherwise, or unless the Processor is required by law to retain such personal data.

User data is deleted from the user database automatically when 366 days have passed since the system's last processing of login information.

12. Limitation of liability

The Processor shall not be liable for any indirect or consequential damages under this DPA.

The aggregate maximum liability of the Processor to the Controller under this DPA shall be limited to a sum corresponding to 100% of the payments made by the Controller to the Processor for the Service during the previous 12 months.

The Processor does not limit its liability, when such limitation would be unlawful.

13. Term

This DPA enters into force on the date written below and shall continue to be in force until the Processor has ceased to process the Controller's personal data, or until replaced by another agreement between the Parties with regard to the data processing.

14. Dispute resolution and jurisdiction

This DPA shall be subject to the provisions regarding dispute resolution and jurisdiction set out in the Main Agreement.

15. Amendments

We reserve the right to make amendments to this DPA. The amended version will enter into force only after the acceptance by both parties.

Signatures

The Parties below have executed this DPA on the date written below. Electronic delivery of an executed counterpart of a signature page to this DPA by email shall be effective as delivery of a manually executed counterpart of this DPA.

Cloudpoint Oy	**(Customer)**
'Processor'	'Controller'
	
_____	_____
Lauri Kaski	Name
CEO	Title
15.1.2024	Date

ANNEX 1 Description of the Data Processing

1. **Purpose of the processing of Personal Data**

   The Processor shall process personal data on behalf of the Controller for the purposes of providing the Service, to the extent such provision of the Service requires processing of personal data by the Processor. The processing shall be carried out in accordance with the Main Agreement, this DPA, and the instructions given by the Controller.

2. **Categories of Data Subjects**

   The processing of personal data concerns the following categories of data subjects:

   - Students
   - Teachers and other personnel of the Customer that use the Service

3. **Types of Personal Data**

The Processor may process the following types of personal data under this DPA.

- Students', teachers' and other personnel's personal data is being processed in:
  - Edudata Compliance
  - Edudata Compliance Service
  - Edudata Privacy

Roles: Student, Teacher, Teacher+, Draftsman, Decision Maker, Customer Admin

- First name
- Last name
- Email address
- IP-address
- Login data
- Browser details
- Device Data
- 3rd party service login information
- Edudata ID
- language
- User creation date
- User last login
- Profile picture
- Role of the user
- Organization (Customer name) name and domain

4. Duration of the processing of Personal Data

Personal data shall be processed under this DPA for the duration of the Term of the Main Agreement. After the Main Agreement has been terminated or expired, and the Processor has ceased to provide the Service, and has conducted all the actions set out in this Agreement relating to the return and deletion process of personal data. Following this, for a maximum period of 180 days, the Processor shall no longer process or store any Customer personal data, except to the extent the Processor is under a statutory obligation to retain the personal data after the termination of the Main Agreement.

The Controller determines the duration of the processing activities and is responsible for ensuring that personal data is deleted accordingly.

Edudata's data is stored in a Google Cloud Project owned and managed by the Customer's organization. In the project, the data is stored in separate Big Query, Firestore databases. Only system log data is stored in the Edudata.io system from the processing, which is automatically deleted within 30 days.

In case the Customer terminates the use of the Edudata Service, the databases remain under the control and responsibility of the Customer. The Processor will process data only in accordance with this Agreement and only for the duration of the Agreement.

- Edudata log data stored: **30 days**
- User data is deleted from the user database automatically when **366 days** have passed since the last login information was updated to the system
- Third party services log data:
    - **18 months**
- Assessments; decisions and requests related to data protection risk assessments of the application and/or service are stored for **3 years**

When a user logins with an M365 or Google Workspace account into Edudata, the user can request a colleague to give the user a teacher or other required role. If the request is denied or not responded within **30 days**, the user information is deleted from the Edudata user database

- If the request is approved the user role is updated and the **366 days** rule above will be applied.

When the data deletion process has started, system log data will be deleted in 180 days.

5. Subprocessors

- Google Ireland ltd – Applies to all users of EDUDATA Service(s)
- Hubspot – Applies to contact and technical support persons only
- Online Partner – Applies to the customers in partners market area
- Delling Cloud – Applies to the customers in partners market area

6. International transfers

Personal data is stored on servers located in the European Economic Area. As a rule, there are no regular transfers of personal data beyond the EEA.

In case personal data is being transferred outside the EEA by subprocessors to a country that the EU Commission has not determined to have an adequate level of data protection, the basis for transfer shall be in accordance with the Chapter V of the GDPR, such as the Standard Contractual Clauses approved by the EU Commission.

ANNEX 2 Security measures

The Processor shall implement and maintain appropriate technical and organizational security measures designed to protect and preserve the security of personal data.

The Processor shall ensure that any person authorized by the Processor to process personal data (including its staff, agents, subcontractors) shall be under appropriate obligations of confidentiality.

Our internal security measures are documented and reviewed twice in a year. Our staff will regularly participate in data privacy and data security training.

Our office is access controlled, guarded and has 24/7 camera surveillance.
All access to the data environments are controlled by IAM and logged.
All user logins are using enforced 2FA and strong authentication keys (Yubico).

Following security measures are implemented in the software development process;

- Security aspects highlighted in orientation of new employees
- Security-related training provided to developers via Google Cloud certifications
- Access to code repositories only by approval of a senior developer
- Local development only in laptops with encrypted disks
- Peer review to the code
- Regular vulnerabilities check and update of software libraries
- Regular monitoring of news channels about cyber-threats and vulnerabilities
- Documentation

Ownership and management of data warehouses implemented in Google's Cloud Services is the Customer's responsibility. The Customer, as the data controller, is responsible for taking the appropriate security measures.

The service is hosted in Google’s Cloud Service. Google employs various security measures in respect of its Cloud Services. More information about Google Cloud Services and the security measures employed Security whitepapers | Google Cloud.