

SCHEDULE E - GDPR Extension - DATA PROTECTION FOR EUROPEAN UNION AND UK USERS

This Schedule extends section 3.3 Personal Information of the DigitalEd Master Service Agreement to cover European Union and UK users.

DEFINITIONS:

Applicable Laws	all national, supranational, foreign or local laws (including case law), legislation, European and UK regulations, statutes, statutory instruments, rules, regulations, edicts, by-laws or directions or guidance from government or governmental agencies including any rules, regulations, guidelines or other requirements of relevant regulatory authorities which have the force of law;
Controller	shall have the meaning given to it in the Regulation;
Data	shall mean the Personal Data and Special Personal Data provided by or on behalf of YOU to DigitalEd pursuant to the Agreement or entered by YOU into the Software or otherwise generated by the Software;
Data Subject	shall have the meaning given to it in the Regulation;
Personal Data	shall have the meaning given to it in the Regulation;
Processing	shall have the meaning given to it in the Regulation;
Processor	shall have the meaning given to it in the Regulation;
Regulation	means the regulations on the protection of natural persons with regard to the processing of personal data and on the free movement of such data known as the General Data Protection Regulation for the EU and the UK
Regulator	means the supervisory authority in the jurisdiction in which YOU are based or which YOU have nominated as YOUR lead supervisory authority (or any replacement or subsequent authority or body which

DigitalEd

	replaces it) and any other regulator who has the power to enforce the Regulation in any territory and who has authority and jurisdiction over DigitalEd and/or YOU;
Services	all services to be provided by DigitalEd under the Agreement;
Special Personal Data	shall mean the special categories of Personal Data as set out in the Regulation;
Sub-Processor	means any third party, including a consultant, sub-contractor, agent or professional adviser or other third party appointed by the Processor which may receive and/or have access to Data.

1 DATA PROTECTION

1.1 The parties acknowledge that YOU are a Controller and DigitalEd is a Processor in relation to the Data.

1.2 To the extent not stated elsewhere in the Agreement, Annex 1 to this Schedule sets out the following information in relation to the Data:

- (a) subject-matter of the Processing;
- (b) duration of Processing;
- (c) nature and purpose of the Processing;
- (d) type of Data; and
- (e) categories of the Data Subjects.

1.3 YOU shall:

- (a) ensure YOU have all necessary rights and consents to Process the Data and to disclose the Data to DigitalEd in accordance with the Regulation;
- (b) provide DigitalEd with YOUR name and contact details (or those of YOUR representative) and the name and contact details of YOUR data protection officer (where one is appointed);
- (c) provide DigitalEd with documented instructions regarding the Processing to be carried out where these exceed the Services;
- (d) be responsible for deciding and determining the following:

- (1) the subject-matter and extent of the Data to be collected and Processed, including which individuals' Data should be Processed;
 - (2) the purpose and manner of Processing of the Data;
 - (3) third parties to whom the Data is disclosed (other than DigitalEd's Sub-processors); and
 - (4) duration of retention of the Data;
- (e) be responsible for the provision of a privacy notice to Data Subjects;
- (f) respond to and implement Data Subject requests to exercise their rights under Articles 15-22 of the Regulation; and
- (g) carry out all data protection impact assessments where required by the Regulation.

1.4 DigitalEd shall:

- (a) Process the Data only on YOUR documented instructions as set out in this Schedule to perform its obligations under this Schedule and if DigitalEd is aware that, or is of the opinion that, any instruction given by YOU breaches the Regulation, DigitalEd shall inform YOU of this were permitted to do so by such law;
- (b) ensure that its personnel who are authorised to Process the Data are under obligations of confidentiality that are enforceable by DigitalEd;
- (c) implement appropriate technical and organisational measures to ensure a level of security appropriate to protect the Data, including from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access;
- (d) taking into account the nature of the Processing, assist YOU with YOUR obligations to comply with Data Subjects' requests and Data Subjects' rights under Chapter III of the Regulation through the use of appropriate technical and organisational measures to the extent that YOU cannot access the Data required using the functionalities available on the Software where such assistance will be charged at DigitalEd's standard rates;
- (e) taking into account the nature of processing and the information available to DigitalEd, assist YOU in ensuring compliance with the YOUR obligations in Articles 32- 36 of the Regulation including:
 - (1) notifying YOU within 48 hours if DigitalEd becomes aware of a breach of the Regulations in relation to the Data and/or if it becomes aware of a breach of the provisions of this Schedule by DigitalEd, any Sub-Processor or any third party; and
 - (2) providing full details of the relevant breach were caused by DigitalEd or any Sub-Processor of the Regulation without undue delay, or where not possible to

DigitalEd

provide all details straight away, to provide such information in phases when it is known;

(f) destroy the Data (including all copies of it) at any time upon YOUR request or upon termination or expiry of this Agreement unless any Applicable Law requires DigitalEd to continue to store the Data or unless YOU require DigitalEd to return the Data in a format to be agreed between the parties;

(g) no more than once per year upon YOUR request, provide a report by an independent auditor to demonstrate DigitalEd's compliance with this Agreement. To the extent that YOU reasonably require further evidence to demonstrate compliance with this Agreement, no more than once per year and on no less than 30 days' notice, DigitalEd will provide YOU or your nominated representative with reasonable access to premises at which the Services are performed and reasonable access to personnel to conduct audits of DigitalEd's compliance with this Schedule and the processing of Data under this Agreement, subject to DigitalEd's confidentiality obligations to its other clients;

(h) not Process or transfer Data outside of the European Economic Area (or any country deemed adequate by the European Commission pursuant to the Regulation) without YOUR prior written consent and without putting in place adequate protection for the Data to enable compliance by YOU and DigitalEd with the obligations under the Regulation; and

(i) promptly provide assistance with responding to any enquiry made, or investigation or assessment of Processing under this Schedule initiated by a Regulator.

1.5 Without prejudice to the restrictions in Clause 1.6 of this Schedule, DigitalEd shall put in place in writing with any Sub-Processor, contractual obligations which are at least equivalent to the obligations imposed on DigitalEd pursuant to Clause 1 of this Schedule.

1.6 YOU consent to the appointment by DigitalEd of Sub-Processors provided that:

(a) DigitalEd notifies YOU in writing of each Sub-Processor prior to the Processing of any Data by the relevant Sub-Processor and shall notify YOU in writing of any change in identity of a Sub-Processor from time to time; and

(b) DigitalEd shall put in place with any Sub-Processor, written contractual obligations which are at least equivalent to the obligations imposed on DigitalEd pursuant to Clause 1 of this Schedule.

(c) DigitalEd shall remain fully liable to CU for the performance of any subprocessor

1.7 In case the terms of this Schedule conflict with the terms of this Agreement, the terms of this Schedule shall apply.

Annex 1 TO SCHEDULE E

Description	Details
Subject matter of the Processing	Provision of STEM (Science, Technology, Engineering & Math) software to enable students to take assessments.
Duration of the Processing	From commencement and until termination or expiry of the Agreement
Nature and purposes of the Processing	Allowing users access to our STEM software for collaboration, and remote storage of user created content. Making records of students and teachers available to students, teachers and customers for academic assessment.
Type of Data	<p>Name (first and last), password, student id, exam results, examiners' comments, and instructor created documents and assessments.</p> <p>For an LTI configuration, we will only have Name (first and last) email address and role.</p>
Categories of Data Subject	Students, teachers, educators, staff and faculty
Description of the Processing	DigitalEd may monitor and compile any anonymized statistical data based upon Customer's and End Users' use of the Service, which may be combined with data from other customers of the Service, but always in an aggregate and anonymous manner to derive statistical and performance information related to the provision and operation of the Service (collectively, the "Analytical Data"). In no event shall the Analytical Data contain any Personal Information. Analytical Data shall only be used for analysis and research purposes, such as providing statistical and performance information to Instructional Users, to improve the Service or for internal analysis and research purposes.
Processing Objectives	Möbius collects data that shall only be used for either functional usability by the platform and analysis and research purposes, such as providing statistical and performance information to Instructional Users, to improve the Service or for internal analysis and research purposes.

DigitalEd

Personal Data	<p>Depending on the setup , Möbius will need to collect student and faculty members first and last names, email address, and student Id.</p> <p>Faculty members will have the option of creating courses and assessments. This content can then be used by the students and graded. Möbius will record these grades for the students and faculty as well as faculty comments.</p>
Backups	<p>Möbius contains all of the data ever created by the school and this data is stored in a school specific private database. This database is backed up every day, this backup is kept for 1 year.</p>
Log data retention	<p>Log data kept for 1 year</p>
Erasure	<p>All database backups are destroyed within 30 days of contract termination. During this period the school can request a copy of the last database backup for archiving purposes.</p>
Data location	<p>All EU and UK data is stored in a Google Cloud data centre in Frankfurt Germany. The data does not leave this centre. Access to the data is described below.</p>
Details of the security measures taken by the Processor	<p>Details of the security measures taken by the Processor:</p> <p>DigitalEd follows the security guidelines as defined by Service Organization Control (SOC 2)</p> <p>Software access to hosted instances is granted securely to Möbius development and support staff in order to set up and maintain software. All access is granted/revoked based on “Need to know” best practices. Our tools handle access to instances through enforcement of public RSA keys that are created by the users needing access. Employees are required to use unique credentials when conducting administrative functions.</p> <p>The data is held in a database dedicated to a single school, this ensures data isolation between schools. Databases are partially encrypted (e.g. passwords) but not all table information is fully encrypted. The data is encrypted when stored at rest</p> <p>Data is destroyed 1 month after the contract has been terminated. This includes the database and all of the</p>

DigitalEd

	<p>backups.</p> <p>DigitalEd is implementing CSA STAR Level 1 from the Cloud Security Alliance CloudSecurityAlliance.org Level 1 Self Assessment: https://cloudsecurityalliance.org/star/levels/</p> <p>GDPR https://www.udemy.com/course/eu-gdpr-data-protection-employee-awareness/</p> <p>FERPA https://studentprivacy.ed.gov/resources/responsibilities-third-party-service-providers-under-ferpa</p> <p>PIPEDA https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/</p>
Data Safeguards	<p>All data is encrypted while in transit (from browser to our service) as well as between services within our data centre and at rest. Data in transit is protected by the Transport Layer Security v 1.3 (SSL/TLS) and data at rest is encrypted using the Advanced Encryption Standard (AES) 256.</p> <p>All systems have their default passwords changed and only the required ports are open.</p> <p>Mobius undergoes a yearly independent 3rd party penetration and vulnerability test to ensure it is secure against intruders from the inside and outside of the application.</p>
Subprocessors	<p>DigitalEd will ensure that the Sub-Processor (listed below) will protect data by following and enforcing the GDPR.</p>
Frequency of audits	<p>Based on the provided above, DigitalEd recommends that once every year and no later than December 31, the Processor will provide the Controller with a report issued by an internal audit on compliance.</p>

Annex 2 TO SCHEDULE E

Type of data collected, who has access to it and the type of process it undergoes.

Categories of the Processor's Employees (positions/groups of positions) who Process Personal Data	(category of) Personal Data that are processed by Employees	Type of Processing	Country of Processing
1. Product Management	Only view anonymized data	In no event shall the Analytical Data contain any Personal Information. Analytical Data shall only be used for analysis and research purposes, such as providing statistical and performance information to Instructional Users, to improve the Service or for internal analysis and research purposes.	Canada
2. Software Developers	First, last names, email address, student ID, any grades that may have been recorded from the use of assignments.	Able to view the raw data stored in the database. The developers have been granted this access which is a higher level than the support or product management levels. This level of access is granted by request and is time limited. All requests are reviewed before approval and are tracked.	Canada
3. Site Reliability Engineers.	First, last names, email address, student ID, any grades that may have been recorded from the use of assignments.	Able to view the raw data stored in the database. The developers have been granted this access which is a higher level than the support, product management or developer levels. This allows these employees to ensure systems are backed up	Canada

DigitalEd

		nightly and routine software upgrades and maintenance can occur.	
4. Customer Success	First, last names, email address, student ID, any grades that may have been recorded from the use of assignments.	It may be required to look at personal information to help solve a problem that a student or faculty member may have encountered. Support has the lowest level of access. This access is secure access that is surfaced within Möbius administration platform.	Canada, UK, Australia
Key Accounts Manager	First, last names, email address, student ID, any grades that may have been recorded from the use of assignments.	It may be required to look at personal information to help solve a problem that a student or faculty member may have encountered. Support has the lowest level of access. This access is secure access that is surfaced within Möbius administration platform.	

Sub-processor engaged by the Processor for the Processing of Personal Data	(category of) Personal Data processed by the Sub-processor	Type of Processing	Country of Processing	Country where Sub-processor's registered office is located
Google	Although we use Google (GCP) it is only for hosting purposes and for the management of the hardware. At no time do we share passwords and secrets with Google nor do we contract Google employees to perform work on our systems.	Hardware and Storage	Germany (Frankfurt)	Germany, USA.

DigitalEd

	In addition, all appropriate agreements have been signed with Google to ensure they know we have EU/UK citizen data and the GDPR must be upheld and enforced.			
AWS	Final backup retrieval at contract termination, secure download. At no time does AWS have the password to this system or the file containing your data.	Storage	Germany (Frankfurt)	Germany, USA
Edufide - Mobius Grading only	First, last name, email address of faculty and students. Exam questions and student answers.	Collecting, Recording, Organising, Structuring, Storage,, Modifying,E rasing, and destroying data	EU, UK	Canada

Please note that Google and AWS are US based companies however the data for all EU and UK customers is stored in Germany(Frankfurt) and does not leave the data centre for any reason without written consent from the customer.

Annex 3 TO SCHEDULE E

Data transfer details at contract termination.

Transfers

Description of the transfer	Entity transferring the Personal Data + country	Entity receiving the Personal Data + country	Transfer mechanism	
Contract Termination	DigitalEd (Waterloo, Canada)	DigitalEd (AWS Frankfurt Germany)	SSL/TLS 1.3 secure file copy	Final transfer of data for customer download on contract termination (Only if the customer requests a copy of the data).

DigitalEd

DigitalEd confirms that its online learning and assessment platform is SOC 2 Type 1 certified. Upon request, DigitalEd will provide a summary or redacted copy of its current SOC 2 Type 1 report, subject to confidentiality obligations.

