

DATA PROCESSING AGREEMENT

THE PARTIES:

1. **DELFT UNIVERSITY OF TECHNOLOGY**, with registered offices at 2628 CN DELFT, Stevinweg 1, represented by Dr. I.M. Haslinger, who, as Library Director is authorised to sign this agreement,

hereinafter referred to as: **"The Controller"**,

and

2. **Service Provider**, having its registered offices and principal place of business in XXXXXXX, listed in the trade register under number XXXXXXX, legally represented in this matter by Mrs./Mr. XXXXXXX, XXXXXXX, who is authorised to sign this Agreement on behalf of the company, hereinafter **"The Processor"**

1 and 2 referred to individually as: **"the Party"** and jointly: **"The Parties"**

Whereas:

On....., the Parties entered into a Contract concerning the provision, implementation, migration of the data from the current software to the new software, maintenance and support of learning management system Software. In the implementation of this Contract, personal data will be processed by the Processor on behalf of the Controller.

The Controller is committed to the protection of these personal data. For this reason, the Parties are using this Data Processing Agreement (Article 28, paragraph 3 of the General Data Protection Regulation, GDPR) and the associated appendices, i.e.:

- overview of processing of personal data and purposes of processing (Appendix A);
 - overview for processing by sub-processors and transfer to third countries (Appendix B);
 - overview of security measures (Appendix C);
 - **If applicable:** Standard Contractual Clauses (Appendix D);
- in order to stipulate what the Processor is and is not permitted or obliged to do with the personal data;

HEREBY AGREE AS FOLLOWS:

1. General

- a. Terms used in this Data Processing Agreement have the same meaning as in the General Data Protection Regulation (Regulation (EU) No. 2016/679).
- b. In the event of any conflict between this Data Processing Agreement and the Contract, this Data Processing Agreement will take precedence. This means that the Contract and any other conditions agreed may in no way prejudice the rights and obligations pursuant to this Data Processing Agreement.
- c. This Data Processing Agreement is subject to Dutch law. Disputes concerning this Data Processing Agreement will be put to the Court in The Hague, The Hague location.

2. Data processing – and general obligations

- a. All personal data will be regarded as confidential data and treated as such. The Processor is permitted to use the personal data solely for the purposes of implementing the Contract and solely on the instructions of and on behalf of the Controller. An overview of all permitted processing has been included in Appendix A.
- b. The Processor will refrain from using the personal data for its own purposes, for the advantage of or on behalf of third parties or for any other purposes, unless a statutory obligation under applicable law obliges it to do so, in which case the Processor will notify the Controller of that statutory obligation prior to processing, unless applicable law prohibits any such announcement for compelling reasons of general interest.
- c. The Parties will comply with applicable privacy legislation and provide each other back and forth with all necessary cooperation and information in order to meet their statutory duties.
- d. The Controller retains all intellectual and other property rights pertaining the personal data.
- e. If, contrary to that stipulated in this Data Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data, the Processor determines the purposes and means for processing the personal data, the Processor will be deemed to be the Controller for said processing.

3. Confidentiality

The Processor will only reveal personal data to staff members for whom knowledge of the personal data is strictly necessary for the purpose of implementing the Contract, except in cases where other statutory obligations apply to them. The Processor will also guarantee that authorised staff members are bound by a duty of confidentiality and abide by the provisions of this Data Processing Agreement.

4. Security

- a. Pursuant to Articles 28 and 32 of the GDPR, the Processor will take appropriate technical and organisational measures to guarantee a level of security in accordance with the risk. The Processor will ensure that these measures take account of current technology, the cost of implementation, the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of data subject(s). Consideration will also be given to the risks that may result from the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to data transmitted, stored or otherwise processed.
- b. The Processor will lay down its security policy in writing. At the Controller's request, the Processor will provide access to its security policy. Appendix C describes the minimum security measures to be taken by the Processor. Since security risks are continually changing, the Processor will regularly update and improve the security measures taken.

5. Data Protection Impact Assessment

In order to enable the Controller to meet any obligation it may have to conduct a Data Protection Impact Assessment (DPIA), the Processor will notify the Controller at its first request and prior to any processing of personal data, of the following:

- i. a systematic description of the processing envisaged;
- ii. an assessment of the risks to the rights and freedoms of data subjects in view of the nature, scope, context and purposes of the processing;
- iii. the measures intended to address the risks stated under (ii), including safeguards, safety measures and mechanisms to ensure the protection of the personal data and demonstrate compliance with the GDPR, taking account of the rights and legitimate interests of the data subject(s) and other persons concerned.

6. Sub-processor

- a. The Processor refrains from outsourcing the processing of personal data under this Data Processing Agreement to sub-processors without prior written permission from the Controller. The Controller grants written permission for the use of sub-processors only in the event that this has been explicitly included in Appendix B. In the event of any intended change (addition or replacement) to one or more sub-processors during this Agreement, the Processor provides the Controller with written advance notice of this change and the Controller has the option of objecting to this change.
- b. In the event that the Processor outsources its obligations under this Data Processing Agreement with written permission from the Controller, the Processor must enter into a sub-processing agreement that imposes the same conditions and obligations on the sub-processor as those imposed on the Processor in this Data Processing Agreement, and especially the obligation to provide adequate guarantees concerning the application of appropriate technical and organisational measures. If the sub-processor fails to meet its obligations towards the Processor, the Processor will be fully responsible towards the Controller for the sub-processor's compliance with its obligations under any such sub-processing agreement. The Processor will provide the Controller with a copy of the sub-processing agreement at its first request, from which commercially sensitive information may be omitted.
- c. Dutch law will apply to the provisions concerning the outsourcing of this Data Processing Agreement.
- d. The Processor maintains a list of the sub-processing agreements entered into as part of this Data Processing agreement and notifies the Controller of this. This list will be updated at least once annually. This list will be kept available for the purposes of the supervisory authority.
- e. Only with prior general consent from the Controller the Processor is allowed to process or arrange the processing of personal data in countries outside the EEA or provide personal data to organisations outside the EEA. The Controller makes this permission conditional on the obligation to include Standard Contractual Clauses (SCCs) if no adequacy decision is applicable (Appendix D).
- f. The Processor will remain fully liable vis-à-vis the Controller for the sub-processor's compliance with its obligations if the latter fails to observe its obligations arising from Applicable Law.

7. Requests from data subjects, government and supervisory authorities

- a. Requests from data subjects
At its own cost, the Processor will cooperate fully in enabling the Controller to comply with the requests of data subjects, for example by providing data subjects with access to the personal data of relevance to them, removing, supplementing, transferring, protecting and rectifying personal data and providing evidence that the request has been met. When a data subject submits a request to the Processor, the Processor will refer the data subject to the Controller and will not engage in any discussion of the contents of the request.
- b. Requests from government and supervisory authorities
At no charge and in close consultation with the Controller, the Processor will cooperate fully in any investigations conducted or requests made by government and supervisory authorities concerning the Controller and will provide all information of relevance to this. If the Processor receives a request of this kind addressed to it, it will notify the Controller without undue delay and the Parties will consult on the steps to be taken, unless that is prohibited in view of the nature of the request. In the latter case, the Processor will represent the reasonable interests of the Controller.
- c. In order to safeguard the protection of personal data, the Processor will in that case ensure that it does not provide the government or supervisory authority with more personal data than is strictly necessary in order to meet the public body's request. If it is possible to take action in law against a request to provide personal data or a prohibition on informing third parties exists, the Processor will take full advantage of this.

8. Audit

- a. With the exception of low-risk processing, the Processor is obliged to have an independent external expert conduct an audit at least once every two years on the Processor's organisation in order to demonstrate that the Processor is compliant with the Contract, the Data Processing Agreement, the GDPR and other applicable legislation and regulations concerning the processing of personal data. In the event that Special Categories of Personal Data are processed, the Processor conducts a periodic audit at least once annually. Its findings must be shared with the Controller.
- b. The Controller is entitled to have an audit of the Processor's organisation conducted by an independent external expert in order to demonstrate that the Processor is compliant with the Data Processing Agreement, the GDPR and other applicable legislation and regulations concerning the processing of personal data. The Controller can make use of its right to have an audit of the Processor conducted at its request a maximum of once annually or more frequently in the event of a specific suspicion that the Processor is not complying with the Data Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data.
- c. The Controller provides the Processor with notice of the audit at least 14 (fourteen) days in advance of it. The audit may not cause unreasonable disruption to the Processor's normal business activities.
- d. The cost of the audit conducted at the request of the Controller shall be paid by the Controller unless the audit findings reveal that the Processor has not complied with the Data Processing Agreement, and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data.
- e. If it is determined during an audit that the Processor is not complying with the Data Processing Agreement, and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data, the Processor immediately takes all measures reasonably necessary in order to ensure that the Processor is compliant. The associated costs shall be paid by the Processor.

9. Reporting of data breaches

- a. The Processor will have procedures in place aimed at ensuring the reasonable detection of security incidents and data breaches and taking action in response, including remedial measures. The Processor will provide the Controller with a copy of the relevant procedures at its first request.
- b. In order to enable the Controller to fulfil its notification obligations, the Processor notifies the Controller of any breach of security within 24 hours at the latest. Reports can be submitted to the Controller via databreach@tudelft.nl, or, if relevant, to another contact designated by the Controller during the term of this Data Processing Agreement and must, in any event, include:
 - i. the nature of the breach and, where possible, the categories of data subjects and personal data records concerned and the approximate number of data subjects and personal data records concerned;
 - ii. the name and contact details of the Processor's data protection officer or another point of contact where further information can be obtained concerning the breach;
 - iii. the likely consequences of the personal data breach;
 - iv. the measures for addressing the personal data breach, including, where appropriate, the measures to mitigate its possible adverse effects.
- c. With regard to every breach as referred to under 9a, the Processor will ensure that it provides the Controller with all cooperation that might reasonably be expected from the Processor, including the provision of sufficient information and support relating to investigations by the supervisory authority:
 - i. in order to rectify and investigate the breach and prevent future breaches;
 - ii. in order to limit the impact of the breach on the privacy of data subjects; and/or
 - iii. in order to limit the damage incurred by the Controller as a result of the breach.

- d. The Processor documents any personal data breaches, including the facts concerning the personal data breach, the consequences of it and any remedial measures taken. The Processor provides this documentation to the Controller as soon as it is requested.
- e. Unless legally required to do so, the Processor will not notify the supervisory authority and/or data subjects of a security breach without prior written permission from the Controller.

10. Retention periods

- a. The Processor will not retain the personal data for longer than is strictly necessary and definitely no longer than the term of the Data Processing Agreement, unless storage of the personal data is a legal obligation, in which case the Processor will not retain the personal data for any longer than the period prescribed by law.
- b. Where necessary, the Processor follows the retention instructions given by the Controller.

11. Liability and indemnity

- a. The Processor is liable for any damages arising from or connected with failure to comply with the Data Processing Agreement, and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data.
- b. The Processor indemnifies the Controller with regard to any third-party claims, fines and or measures, including from data subjects and the supervisory authority, made or imposed vis-à-vis the Controller because of a breach of the Data Processing Agreement, and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data by the Processor and/or by persons/legal persons deployed by the Processor, including but not limited to staff members and/or sub-processors.
- c. The Processor arranges adequate coverage for its liability by means of liability insurance. At the Controller's request, the Processor allows the Controller to consult (the policy of) this liability insurance held by the Processor.

12. Change

- a. In the event of an intended change to the processing of personal data, such as the deployment of a new sub-processor, a change in the transfer of personal data to third countries and/or international organisations or changes to the security measures taken, the Processor is obliged to notify the Controller immediately about the intended changes and the Parties will consult as soon as possible on the consequences for this Data Processing Agreement.
- b. The Processor will not be entitled to implement a change until the Controller has issued prior written permission for this change. A change may never result in the Controller no longer being able to comply with the applicable privacy legislation. Any changes will be recorded in writing in Appendix B.
- c. In the event of any change to the current policy rules of the supervisory authority, the Parties will make use of Appendix C to implement the changes required in order to comply with the new policy rules.

13. Duration and termination

- a. The duration of the Data Processing Agreement is identical to that of the Contract. The Data Processing Agreement cannot be terminated prematurely or separately from the Contract.
- b. The Parties have agreed that, within one month of the termination of the Data Processing Agreement, the Processor destroys, return and/or transfer (to be chosen by the

Controller) all personal data and copies it has processed, some of which may be held by persons/legal persons deployed by the Processor, including but not limited to staff members and/or sub-processors, and provides written confirmation of this to the Controller, unless the law prohibits return or destruction. In the latter event, the Processor guarantees that it will observe confidentiality with regard to the personal data processed and will no longer actively process the personal data.

- c. The Processor bears the costs of destruction, return and/or transfer of the personal data. The Controller is at liberty to set more detailed requirements concerning the manner of destruction, return and/or transfer of the personal data, including with regard to the file format.
- d. When this Data Processing Agreement terminates, the provisions that are intended to continue to apply after it will remain in force, such as Article 2 (ownership), Article 3 (confidentiality) and 11 (liability).

AGREED AND SIGNED:

Delft University of Technology

Dr. I.M. Haslinger

Library Director

Date:

Company name

MR/Mrs. xxxxxxxxxxxx

Function

Date:

Appendix A **Personal data**

Processing Description of the subject and duration of the processing	Purposes Description of the nature and objective of the processing	Categories Description of the categories of data subjects	Personal data Description of the type of personal data being processed
<i>[Description of the processing activities/ brief notes on the services and the time period in which or date until when the processing will be carried out]</i>	<i>[Describe the type of processing here, e.g.: storing, amending, deleting, etc. And the purposes of the processing]</i>	<i>(E.g.: students, staff members, research participants, etc.)</i>	<i>[E.g.: name, address, postcode, telephone number, email address, age, gender, education, debts, etc.]</i>

Appendix B Permission for processing personal data by sub-processors and transfer to third countries

- **Sub-processors**

The Controller hereby grants permission to the Processor for the deployment of the sub-processors referred to below [*to be completed by the Controller and Processor*]:

Sub-processor deployed by the Processor to process personal data	(Category of) personal data to be processed by sub-processor	Type of processing	Country of processing	Country in which sub-processor is based

- **Transfer**

The Controller grants the Processor permission for transfer to third countries/international organisations [*to be completed by the Controller*]:

Description of transfer	Entity transferring the personal data + country	Entity receiving the personal data + country	Transfer mechanism (e.g. SCC)

Appendix C **Security measures**

[This is a list of security measures with examples. To be completed jointly by the Parties]

- **List of security measures**

Policy and organisation Security policy Risk analysis Awareness-raising Change management Continuity management Confidentiality
Access security Physical access security Logical access security Life-cycle user accounts Authorisation policy (allocation of no more rights than necessary, withdrawal of rights)
Management of vulnerabilities and anti-malware
Confidentiality and data integrity Privacy policy (End-to-end) encryption What measures are taken to ensure that the transport and storage of the data takes place securely Back-up/restore provisions
Incident response, reporting and remediation
Patch management
Auditing and logging Ensuring secure logging (Periodic) audits by third parties
Software development OWASP Top 10 security risks OWASP Top 10 Proactive controls Peer review/code review Security test (penetration test)

The Processor holds the following certificates (if applicable), for which the Processor itself is responsible for any renewals, ensuring that the Processor holds a valid certificate throughout the term of this agreement:

Name of certificate	Organisational unit/service to which the certificate relates	Certificate's period of validity	Declaration of applicability

- Specific instructions concerning data retention

Duration of processing	Duration of storage/back-up	The chosen method of data destruction
		• Removal • Anonymisation • Pseudonymisation