Data Processing Agreement

1. Data Protection

1.1 Arrangement Between the Parties

1.1.1 The Parties each acknowledge and agree that the factual arrangements between them dictate the classification and role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, the Parties anticipate that, in respect of the Customer Data, as between the Customer and the Supplier for the purposes of this Contract, the Customer shall act as the Controller and the Supplier is appointed by the Customer to and shall act as the Processor in accordance with the terms of this Schedule 2.

1.1.2 Each of the Parties acknowledges and agrees that Appendix A (Data Processing Particulars) to this Contract is an accurate description of the Data Processing Particulars.

1.1.3 Notwithstanding Paragraph 2.1.1 if either Party is deemed to be a joint Controller with the other in relation to the Customer Data, the Parties agree that they shall:

(a) be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations where Customer Data has been transmitted by it, or while Customer Data is in its possession or control; and

(b) acting reasonably and in good faith seek by way of variation or additional agreement or arrangement, to document the parties' respective obligations in accordance with Data Protection Laws (particularly in respect of communications with Data Subjects, third parties and a Regulator, including in respect of transparency requirements and notification obligations).

1.1.4 Each Party agrees that in performing its obligations under this Contract, it shall comply with the obligations imposed on it under the Data Protection Laws.

1.2 **Contact Data**

1.2.1 Notwithstanding Paragraph 2.1. the Parties each acknowledge and agree that they may need to Process Personal Data in relation to each Party's representatives (in their respective capacities as Controllers) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Contract and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with their respective regulatory obligations.

1.2.2 Each Party shall Process such Personal Data for the purposes set out in Paragraph 2.2.1 in accordance with their respective privacy policies. The Parties acknowledge that they may be required to share Personal Data with members of their Group and other relevant parties, within or outside of the country of origin, in order to carry out the activities listed in Paragraph 2.2.1, and in doing so each Party will ensure that the sharing and use of this Personal Data complies with applicable Data Protection Laws.

1.3 **Data Processor Obligations**

1.3.1 In relation to any Data that the Customer provides or makes available to the Supplier or that the Supplier Processes for and on behalf of the Customer (the Customer acting as the Controller) the Supplier shall:

(a) only Process the Customer Data for and on behalf of the Customer for the purposes of performing its obligations under this Contract, and only in accordance with the terms of this Contract, any Data Transfer Agreement (where applicable) and any documented instructions from the Customer (unless required to do otherwise by Applicable Law, in which case it shall (unless prohibited from doing so by such Applicable Law) inform the Customer of such legal requirement before Processing);

(b) undertake any Processing of the Personal Data it carries out on behalf of the Customer in accordance with the terms of this Contract;

(c) unless prohibited by Applicable Law, notify the Customer immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that any of the Customers instructions under Paragraph 2.3.1(a) infringe any of the Data Protection Laws;

take, implement and maintain appropriate technical and organisational security measures which are sufficient to comply with the obligations imposed on the Customer by the Security Requirements; and at any time where requested provide to the Customer evidence of its compliance with such requirements promptly, and in any event within forty-eight (48) hours of the request;

(d) hold the Customer Data in such a manner that it is capable of being distinguished from other data or information processed by the Supplier;

(e) only disclose Customer Data to its Personnel who are required to assist it in meeting its obligations under this Contract and ensure that no other Personnel shall have access to such Customer Data;

(f) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who shall have access to the Customer Data, and ensure that each member of its Personnel shall have entered into appropriate contractually-binding confidentiality undertakings and that they receive periodic data security and privacy training. Such persons include those who Process the Customer Data or whose roles relate to procuring, developing and/or maintaining technical infrastructure or tools used to Process the Customer Data;

(g) within thirty (30) calendar days of a request from the Customer, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the Customer (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Schedule 2 (Data Protection), and provide reasonable information, assistance and co-operation to the Customer, including access to relevant Personnel and/ or, on the request of the Customer, provide the Customer with written evidence of its compliance with the requirements of this Schedule 2 (Data Protection);

(h) subject to Paragraph 2.3.1(k) not disclose Customer Data to a third party (including a Sub-Processor or any Group company or affiliate, or any Data Importer) in any circumstances without the Customer prior written consent, save in relation to:

(i) transfers made pursuant to Paragraph 2.4 (Appointing Sub-Processors) and/or Paragraph 2.5 (International Transfers) of this Contract; and/or

(ii) Third Party Requests in which case it shall comply as applicable with the terms of Paragraph 2.6;

(i) promptly comply with any request from the Customer to amend, transfer or delete any Customer Data;

(j) notify the Customer promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or Regulator Correspondence and shall:

(i) not respond to or disclose any Customer Data in response to any Data Subject Request or Regulator Correspondence without first obtaining the Customers prior written consent; and

(ii) provide the Customer with all reasonable cooperation and assistance required by the Customer in relation to any such Data Subject Request or Regulator Correspondence;

(k) notify the Customer promptly (and in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected or threatened Personal Data Breach in relation to the Customer Data ("Data Loss Event") (and follow-up in writing) and shall, within such time scale specified by the Customer (acting reasonably and in good faith):

(i) seek to recover the compromised data as soon as practicable and implement any measures necessary to restore the security of the compromised Personal Data;

(ii) promptly provide the Customer with a report containing details about the nature of the Data Loss Event and provide the Customer further information as details become available;

(iii) investigate the incident and its cause;

(iv) assist the Customer to make any notifications to the Regulator and affected Data Subjects; and

(v) not make any public statements relating to the incident without the prior written approval of the Customer;

(l) provide the Customer with reasonable assistance to comply with the obligations imposed on the Customer by the Data Protection Laws, including:

(i) compliance with the Security Requirements;

(ii) obligations relating to notifications required by the Data Protection Laws to the Regulator and/ or any relevant Data Subjects;

(iii) undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the Regulator and/or any other relevant regulatory body in respect of any such Data Protection Impact Assessments); and

(iv) without undue delay and where feasible not later than seventy-two (72) hours after having become aware of it notify Personal Data Breaches to the Regulator and/or any other relevant regulatory body unless the Personal Data Breach is

unlikely to result in a risk to the rights and freedoms of natural persons;

(m) not, whether by act or omission, cause the Customer to breach any of its obligations under the Data Protection Laws;

(n) comply with the obligations imposed upon a Processor under the Data Protection Laws and to the extent that the Processor is subject to Applicable Law which requires a higher level of protection for Personal Data than the Data Protection Laws, also comply with such Applicable Law; and

(o) upon the earlier of:

(i) termination or expiry of this Contract or the relevant Data Transfer Agreement (as applicable); and

(ii) the date on which the Customer Data is no longer relevant to, or necessary for, the provision of the Services,

cease Processing all Customer Data and return and/or permanently and securely destroy the Customer Data and all copies in its possession or control (such that the Customer Data is no longer retrievable), as directed in writing by the Customer and, where requested by the Customer, certify that such destruction has taken place (promptly, and in any event within [forty-eight (48)] hours of the request) except to the extent required by Applicable Law to retain the Customer Data;

1.3.2 Except as otherwise provided, this Contract does not transfer ownership of, or create any licences (implied or otherwise), in any intellectual property rights in any Personal Data.

1.4 Appointing Sub-Processors

1.4.1 The Supplier shall not subcontract the performance of any of its obligations under this Contract without the prior written consent of the Customer;

1.4.2 The Supplier shall be permitted to appoint a sub-contractor to perform any of its obligations under this Contract which include the Processing of the Customer Data ("**Sub-Processor**") in accordance with this Paragraph 2.4 and to disclose Customer Data to such Sub-Processor for Processing in accordance with the Supplier's obligations under this Contract (acting as a Processor or Sub-Processor only), provided always that:

(a) the Supplier undertakes thorough and appropriate due diligence on the proposed Sub-Processor demonstrating the ability to provide sufficient guarantees under the Data Protection Laws, including a risk assessment of the information governance-related practices and processes of the proposed Sub-Processor, which shall be used by the Supplier to inform any decision on appointing the proposed Sub-Processor;

(b) the Supplier provides the Customer with full details in writing of the proposed Sub-Processor (including the results of the due diligence undertaken in accordance with Paragraph 2.4.1(a)) before its appointment and the Customer has consented to such appointment in writing, the Customer having at the date of this Contract consented to the appointment of the Sub-Processors identified in Appendix A; and

(c) the Sub-Processor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Schedule 2 (Data Protection);

1.4.3 Notwithstanding any consent or approval given by the Customer under Paragraph 2.4.1, the Supplier shall remain primarily liable to the Customer for the acts, errors and omissions of any Sub-Processor to whom it discloses Customer Data, and shall be responsible to the Customer for the acts, errors and omissions of such Sub-Processor as if they were the Supplier's own acts, errors and omissions to the extent that the Supplier would be liable to the Customer under this Contract for those acts, errors and omissions.

1.5 **International Transfers**

1.5.1 The Supplier shall not and shall ensure that no Sub-Processor shall make a Restricted Transfer without the prior written consent of the Customer and without taking such measures as are necessary to ensure the transfer is in compliance with Data Protection Laws, including, where required by the Customer, entering into an appropriate Data Transfer Agreement.

1.5.2 Where the Supplier or its Sub-Processor wishes to make a Restricted Transfer the following provisions shall apply:

(a) the Supplier shall submit a written request (at its own cost) to the Customer for its written approval which shall set out the following details:

(i) the intended recipient (Data Importer) and any other parties with whom Customer Data would be shared;

(ii) the proposed Customer Data which will be transferred and/or Processed;

(iii) the proposed country or countries to which Customer Data will be transferred and/or Processed in;

(iv) the proposed transfer, including duration, scale and regularity of the transfer, the length of any onward Processing chain and the number of actors involved and the transmission channels;

(v) information on the Applicable Laws of the importing country(ies) which apply to the Data Importer and practices of the importing country(ies) which could potentially impinge on the Data Importer's ability to meet the terms of the Data Transfer Agreement, along with information on the Data Importer's process in responding to a Third Party Request;

(vi) without limiting Paragraph 2.5.2(a)(v), how the Supplier will ensure that the Data Subjects have enforceable rights and effective legal remedies;

(vii) any Government Access made to the Data Importer or those third parties with whom the Data Importer may/shall onward share Customer Data; and

(viii) the results of a Data Protection Impact Assessment (where applicable).

(b) In seeking such approval the Supplier shall ensure that it has regard to and complies with current government and Regulatory policies, procedures, guidance and codes of practice on, and any approval processes in connection with the Processing and transfers of Personal Data to a Restricted Country.

(c) If any of the requirements in Paragraph 2.5.2(a) and/or (b) cannot be met no Restricted Transfer shall be permitted.

(d) Where consent is granted by the Customer pursuant to Paragraph 2.5.2(a), the Supplier shall comply with such other instructions and shall carry out such other actions as the Customer may notify in writing, including without limitation:

(i) the execution by the Customer (as Data Exporter) and the Supplier (as Data Importer) of a Data Transfer Agreement and the incorporation of such Data Transfer Agreement into this Contract; or

(ii) in the case of a Sub-Processor acting as Data Importer, the Supplier procuring that the Data Importer at the Customer's option:

(1) enters into a data processing agreement direct with the Customer on such terms as may be required by the Customer or with the Supplier on terms which are equivalent to those agreed between the Customer and the Supplier relating to the relevant Customer Data transfer (save that the Sub-Processor shall have no right to transfer the Customer Data to any other third party or otherwise transfer the Customer Data outside of the recipient country except for transfers back to the Customer); and

(2) enters into a Data Transfer Agreement with the Customer or the Supplier (as Data Exporter); and

(3) adopts such technical and organisational measures which the Customer deems necessary for the purpose of protection of the Customer Data and

ensuring that the Data Subjects have enforceable rights and effective remedies.

(e) Where consent is granted by the Customer pursuant to Paragraph 2.5.2(a), the Supplier shall ensure there are no changes to the Processing locations or onwards transfers of Customer Data to any other locations, without seeking the Customers prior written consent in accordance with this Paragraph 2.5 which may be subject to such measures as the Customer deems necessary for the purpose of protecting the Customer Data and ensuring that the Data Subjects have enforceable rights and effective remedies.

(f) The Supplier agrees that any liabilities, costs, expenses, damages and losses incurred by the Customer as a result of a breach of any Data Transfer Agreement by a Data Importer (a "Data Export Loss") will be recoverable by the Customer from the Supplier as if such Data Export Loss had been caused by the Supplier's own acts or omissions.

1.5.3 Nothing in this Contract is intended to undermine or conflict with any terms of the relevant Data Transfer Agreement. In the event of any conflict, the terms of the Data Transfer Agreement shall prevail.

1.6 Third Party Requests

1.6.1 Where the Supplier or any Sub-Processor or any of their Sub-Processors, in each case who receive Customer Data as part of a Restricted Transfer, or any other third party recipients of Customer Data receive a Third Party Request or becomes aware of Government Access in relation to Customer Data transferred to it (the **"Receiving Party"**), the Supplier shall, unless prohibited by Applicable Law from doing so, promptly (and in any event within forty-eight (48) hours) notify the Customer and provide all information available to it

(including in the case of a Third Party Request, the requesting authority, legal basis for the request and any initial response provided).

1.6.2 Where the Receiving Party is prohibited by Applicable Law from notifying the Customer of a Third Party Request or Government Access, it shall use its best efforts to obtain a waiver of the prohibition to notify the Customer and communicate to any entity requesting such disclosure the following message: “The information you wish to access is the legal responsibility of (“the Controller”). The Controller requests in the strongest terms that, before any further steps are taken, you consult the Controller urgently by contacting the Controller’s Data Protection Officer".

1.6.3 In the event of a request or access referred to in Paragraph 2.6.2, the Receiving Party shall:

(a) review the legality of the request and exhaust all remedies to challenge the request if it concludes there are grounds under the Applicable Law of the country of receipt to do so. No disclosure shall be made until required under applicable procedural rules;

(b) document its assessment and challenge of the request for disclosure and to the extent permitted under the Applicable Law of the Data Importer make this available to the Customer and a Regulator promptly upon request from the Customer; and

(c) only provide the minimum amount of information possible, based on a reasonable interpretation of the request, including, without limitation, redacting any of the Customer’s confidential information and Customer Data which is not necessary for the purposes of the request.

1.6.4 In any event, if the request is made to a Data Importer, which as a result of the Third Party Request is no longer able to comply with the Data Transfer Agreement, the Supplier shall and shall procure that any Sub-Processor shall notify the Customer of such inability.

1.6.5 The Supplier shall ensure the obligations set out in Paragraphs 2.6.1 to 2.6.4 are included within the applicable data processing or sharing agreements it has with any other Receiving Party.

1.6.6 Where the Supplier reasonably believes it is obliged under Applicable Law or a Data Transfer Agreement to notify a Regulator or Data Subjects of any Third Party Request or any other compliance breach under Data Protection Laws, the Supplier shall seek the prior written consent of the Customer (which shall not be unreasonably withheld).]

1.7 Notwithstanding anything in this Contract to the contrary, this Schedule 2 (*Data Protection*) shall continue in full force and effect for so long as the Supplier Processes any Personal Data.

2. RECOVERABLE LOSS AND COMPENSATION

2.1 The provisions in this Contract shall not prevent the Customer from recovering any Losses it incurs in relation to:

2.1.1 legal fees, on a solicitor/client basis;
2.1.2 other professional charges and expenses;
2.1.3 disbursements;
2.1.4 costs of investigation including forensic investigation;
2.1.5 cost of breach notification, including notifications to Data Subjects, Regulator(s) or any other parties including listing authorities whether notification is required under Applicable Law or otherwise made in the reasonable belief that notification is necessary;

2.1.6 cost of complaints handling, including providing Data Subjects with credit and/or fraud monitoring services and/or credit reference checks, setting up contact centres (e.g. call centres), and making ex gratia payments;

2.1.7 costs of claims;

2.1.8 cost of litigation;

2.1.9 costs of settlement, including ex gratia payments;

2.1.10 judgement interest; and

2.1.11 penalties, including fines.

2.2 To the extent that the Supplier has an entitlement under Data Protection Laws to claim from the Customer compensation paid by the Supplier to a Data Subject or third party as a result of a breach of Data Protection Laws (in full or in part) by the Customer, the Customer shall be liable only for such amount as directly relates to the Customer's responsibility for any damage caused to the relevant Data Subject or third party. For the avoidance of doubt the Customer shall only be liable to make payment to the Supplier under this Clause 3.2, upon receipt of evidence from the Supplier, which shall be to the Customer's reasonable satisfaction and that clearly demonstrates:

2.2.1 that the Customer has breached Data Protection Laws;

2.2.2 that such breach contributed (in part or in full) to the harm caused entitling the relevant Data Subject or third party to receive compensation in accordance with Data Protection Laws; and

2.2.3 the proportion of responsibility for the harm caused to the relevant Data Subject or third party which is attributable to the Customer.

3. INDEMNITY

3.1 The Supplier shall indemnify on demand and keep indemnified and hold harmless the Customer from and against:

3.1.1 any monetary penalties or fines levied by any Regulator on the Customer;

3.1.2 the costs of any investigative, corrective or compensatory action required by a Regulator, or of defending any proposed or actual enforcement taken by a Regulator including if such investigation arises as a result of a self-report or otherwise;

3.1.3 any Losses suffered or incurred by, awarded against, or agreed to be paid by, the Customer pursuant to a claim, action or challenge made by a third party against the Customer (including by (or on behalf of) a Data Subject); and

3.1.4 except to the extent that Paragraphs 4.1.1 and/ or 4.1.2 and/ or 4.1.3 apply, any Losses suffered or incurred, awarded against, or agreed to be paid by, the Customer,

in each case to the extent arising as a result of a breach by the Supplier (or its Sub-Processors) of this Contract and/or their respective obligations under the Data Protection Laws.

3.2 Nothing in this Contract will exclude, limit or restrict the Supplier's liability under the indemnity set out in Paragraph 4.1.

4. INSURANCE

4.1 The Supplier agrees:

4.1.1 to obtain and keep in full force and effect at all times a policy or policies of insurance which meet(s) the following conditions:

(a) it must cover liability for damage arising to any person;

(b) it must apply in relation to the Processing of the Customer Data; and

(c) it must have policy limits and provisions conforming to such requirements as the Customer may from time to time reasonably prescribe;

4.1.2 to deliver to the Customer:

(a) copies of all applicable insurance policies taken out pursuant to the provisions of this Contract (to the extent permitted by the insurance conditions); and

(b) evidence of premiums paid in relation to such insurance;

4.1.3 to ensure that the Customer shall be entitled to the benefit under such insurance and that the Customer's interest will be noted on the policy; and

4.1.4 to not do, or omit to do, anything to vitiate either in whole or in part any of the insurance cover that it is obliged to have and maintain under this Paragraph 5. The Supplier must notify the Customer immediately if the insurance cover set out in this Paragraph 5 lapses or is denied.

5. TERMINATION

5.1 In the case of any non-compliance by the Supplier or any Sub-Processor with any of the obligations under this Schedule 2, the Data Protection Laws, and/or the Customer's instructions, the Customer may, by giving written notice to the Supplier unilaterally:

5.1.1 immediately terminate this Contract; and/or

5.1.2 suspend any Personal Data submission or sharing under this Contract; and/or

5.1.3 require the Supplier to cease or suspend any Processing of Customer Data including in specific locations or by specific Sub-Processors.

6. AMENDMENTS

6.1 The Parties acknowledge that at the date of this Contract, the Data Protection Laws are subject to change and consultation, Regulatory guidance consultations in respect of Data Transfer Agreements, associated supplementary measures to ensure international transfer rights and compliance matters arising under Articles 28, 46 and 47 of the GDPR/US GDPR. The Parties acknowledge it may be necessary for the Customer unilaterally to amend this Contract, upon written notice to the Supplier, to ensure the Customer's continued compliance with Applicable Law.

6.2 If at any time, in the Customer's opinion, it needs to amend this Contract in order to comply with its obligations under Applicable Law, the Supplier agrees:

6.2.1 where permitted by Applicable Law, the Customer may, at any time by giving the Supplier thirty (30) days' notice, unilaterally:

(a) replace or require the replacement of any Data Transfer Agreement entered into in connection with this Contract with any amended or updated version of those clauses approved under Data Protection Laws or other applicable data transfer mechanism which is or may become available (including any standard clauses forming part of an applicable code of conduct or certification scheme) with such details of the transfers as necessary completed by the Customer;

(b) amend this Contract to ensure (in its opinion) that any Restricted Transfers or related Processing comply with Data Protection Laws including further to any judgement of an applicable court or guidance issued by a competent Regulator;

6.2.2 where execution of a document is required under Data Protection Laws:

(a) promptly agree, accede to and/or to enter into an appropriate written variation of this Contract including any Data Transfer Agreement, or to document information or make the amendments which in the Customer's opinion are required; and

(b) If such amendments are not able to be agreed, the Parties acknowledge and agree that no further Processing of the Personal Data (in particular the Customer Data) under this Contract will be carried out until such variation has been agreed and executed.

7. GOVERNING LAW

This Schedule 2 shall be governed by and construed in accordance with Danish Law.

Appendix A – The Services:

1. INTRODUCTION

1.1. The Supplier shall provide the following services to the Customer:

Title	Description
The subject matter and duration of the Processing	The purpose of the data processor's processing of personal data on its behalf of data controllers are: ● To automatically divide the students into groups on the basis of the students information entered in the questionnaire. ● To improve the group formation process offered by the data processor so that it becomes better in later group formations. ● To allow the data controller's contact persons to carry out the tasks themselves to some extent using UniHelper's self-service solution called “The Portal”.
The nature and purpose of the Processing	The data processor makes the UniHelper system available to the data controller and thereby stores and processes personal data about the data controller students on the servers of the data processor's sub-processors.

The type of Personal Data being Processed	For the data controller's contact persons: ● Name ● Email ● Correspondence regarding data processing ● Other information necessary for UniHelper to fulfil its contractual obligations or increase the level of service. For the students: ● Name ● Email address ● Study number ● Class/course number ● Expectations for the group work ● Competence profile ● Possibly email correspondences ● Possibly tailored questions selected by the data controller that are not sensitive or confidential in nature. ● Possibly other non-sensitive information that the data controller deems necessary in order for UniHelper to provide their service. Possibly other information of a non-sensitive nature that the student submits, such as answers to evaluation questions.
The categories of Data Subjects	Students who start the program knows the data controller. Data controllers have chosen to use the UniHelper system. Contact persons for data controllers.
Data Retention/Deletion Period and Process	The data processing is time-limited from the time the students start the education, to the end of the trial-period in case the contract won't be extended.
The Supplier will only use the	1. TYPEFORM SL a. CVR no.: i. ESB6583 1836

Approved Sub-Processors listed in this column.	b. Address: i. C/Bac de Roda, 163 (Local), 08018 – Barcelona (Spain) c. Contact Information: i. gdpr@typeform.com d. Description of processing: i. Hosting of questionnaires that the students fill in and forwarding of results. e. Processing locations: i. Typeform makes use of AWS' data centers in the USA. A list of AWS data centres can be seen here. As the service is cloud-based, it is not possible to specify the exact addresses where the data is located. Read more about Security at Typeform here. 2. Scaleway SAS a. CVR no.: i. FR354331 15904 b. Address: i. 8 rue de la ville l'Evêque – 75008 Paris, FRANCE c. Contact Information: i. privacy@scaleway.com d. Description of processing: i. Hosting of UniHelper's services, and storage of the students' data, and data for the data controller's employees. e. Processing locations: i. Scaleway has data centres in many countries in Europe, but we use the PARIS-2 region located in Paris. 3. Proton Technologies AG a. CVR no.: i. CHE-354. 686.492 b. Address

	i. Route de la Galaise 32, 1228 Plan-le s-Ouates, Geneva, Switzerland c. Contact Information i. gdpr@protonmail.com d. Description of processing i. Protonmail is used to handle emails that contain personal data on students. e. Processing locations i. Several redundant data centres in Switzerland 4. Flowmailer B.V a. CVR no.: i. KvK62154885 b. Address i. Rotterdam at Van Nelleweg 1, 3044 BC c. Contact Information i. contact@flowmailer.com d. Description of processing i. FlowMailer is used to send out emails in higher quality, for example when the students need to know their groups e. Processing locations i. 3 geographically dispersed data centres in Amsterdam.