

GENERAL TERMS AND CONDITIONS FOR JOINT DATA PROCESSING (ANNEX 1 TO THE STUDENT EXCHANGE AGREEMENT)

concluded by and between

Corvinus University of Budapest (registered address: 1093 Budapest, Fővám tér 8., Hungary, legally represented by Előd Takáts Rector) as data controller (hereinafter referred to as "Data Controller 1"), on the one hand

and

the **contracting University** in the student exchange agreement as data controller (hereinafter referred to as "Data Controller 2"), on the other hand,

(the Data Controller 1 and the Data Controller 2 shall be individually referred to as a "Party" or "Data Controller" and collectively as the "Parties" or "Data Controllers"), subject to the following terms and conditions and with consideration to Article 26 of the GDPR.

1. TERMS

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

'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;

'data processor': means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'data transfer': making data available to particular third party;

'data protection impact assessment': obligation according to Article 35 of GDPR;

'personal data breach': means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'pseudonymisation': means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'recipient': means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities

shall be in compliance with the applicable data protection rules according to the purposes of the processing;

'third party': means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

'GDPR': Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

'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;

'special categories of personal data': personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2. THE DEFINITION OF JOINT DATA PROCESSING

2.1. The Data Controllers agree to these General Terms and Conditions for Joint Data Processing - Student Exchange Agreements (hereinafter referred to as "Data Processing General Terms and Conditions") in order to ensure that the joint data processing activities related to the service provided by the Student Exchange Cooperation Agreement (hereinafter referred to as "the Master Contract") comply with the GDPR. The definition, purpose, legal basis and duration of the joint controller activities carried out by the Parties, the data subjects concerned by such activities, the categories of the personal data concerned and the identity of the processor (if any) shall be determined in Appendix 1 hereof.

3. RIGHTS AND OBLIGATIONS

3.1. The Parties shall jointly determine the purposes and means of the processing as set out in Appendix 1. The Parties agree that the processing will be carried out on an appropriate legal basis and for lawful purposes, with due regard to the principles and provisions of the GDPR on the processing of personal data, the applicable legal rules, this Data Processing General Terms and Conditions and the Master Contract.

3.2. The Parties shall cooperate to ensure the lawful processing of personal data in accordance with this Data Processing General Terms and Conditions, with consideration to the principles governing the processing of personal data.

3.3. In accordance with Article 30 of the GDPR, each Party shall keep a record of the processing activities to be carried out hereunder within its control. Either Party defaulting on or inadequately performing its obligation of record-keeping shall be solely liable for its default or inadequate performance.

3.4. The Parties mutually agree that the documentation relating to the data protection activities subject to this Data Processing General Terms and Conditions shall be managed and stored by Data Controller 1.

- 3.5. The information of the data subject, including, where applicable, the drafting of the data subject's consent form, shall be provided for by Data Controller¹. The storage of the consent forms in a retrievable form for a period of time to be mutually agreed by the Parties shall be ensured by Data Controller¹.
- 3.6. Should it be necessary to involve a data processor to carry out the processing activities set out in this Data Processing General Terms and Conditions, the written contract to be entered into with the processor shall be concluded by Data Controller¹ based on the authorization by Data Controller². The right of instruction of the Data Controllers towards their jointly appointed data processor appointed shall be exercised by Data Controller¹.
- 3.7. The Parties shall guarantee that the persons/employees involved in the data processing shall receive adequate training on data protection and, in particular, they shall warrant that the employees and other persons they shall involve in the performance hereof have sufficient knowledge of the risks associated with the processing of personal data and of the applicable data processing regulations.
- 3.8. The concerned Data Controller shall respond to requests from public authorities regarding the joint processing activities hereunder, following prior notice given to the other Party. The Parties shall cooperate with each other in the performance of requests from public authorities.
- 3.9. In the event a data protection impact assessment is to be carried out in relation to the joint processing hereunder, the Parties shall cooperate prior to the processing in the interest of the performance of such impact assessment.

4. TASKS RELATED TO THE DATA SUBJECTS EXERCISING THEIR RIGHTS RELATED TO JOINT PROCESSING

- 4.1. Data Controller¹ shall inform the data subject of the processing of the personal data in advance or at the time determined in Article 14 of the GDPR.
- 4.2. The Parties shall respond to requests received by them independently, in accordance with the rules of procedure mutually agreed upon by the Parties. Anything contained herein to the contrary notwithstanding, the Parties agree that, with consideration to Article 26 of the GDPR, the data subject may exercise his or her rights against either Data Controller. The Parties shall duly cooperate with each other to respond to the requests from the data subject.
- 4.3. According to the rules of procedure mutually agreed upon by the Parties, each Party shall respond to and perform any request received from data subjects regarding the processing of personal data in accordance with its own rules of procedures. Should the cooperation of the other Party be required to perform the request, the other Party shall comply with the request of the first Party in writing within a reasonable period of time mutually agreed by the Parties, but in no more than 5 working days.

5. PERSONAL DATA BREACH

- 5.1. Either Party becoming aware of a personal data breach in the course of its activities shall inform the other Party of such personal data breach without undue delay, but no later than in 24 hours after becoming aware of the same.
- 5.2. The Parties shall duly cooperate to investigate the cause and remedy the consequences of the personal data breach.

- 5.3. The Parties shall keep appropriate records of the incidents occurring in the course of the data protection activities set out in this Data Protection Agreement within their respective spheres of interest. The liability for any failure to perform such record-keeping obligation properly or at all shall rest solely with the Party in default.
- 5.4. The notification of a personal data breach to the supervisory authority shall be made by the Party where the personal data breach occurred, in agreement with the other Party.
- 5.5. Should it be necessary to inform the data subjects of the personal data breach, the Party where the incident occurred shall inform the data subjects, in agreement with the other Party.

6. LIABILITY

- 6.1. In the event of unlawful processing, the liability shall rest with the Party within the control of whom such unlawful processing occurred.
- 6.2. The Party causing damage to the other Controller or any third party, whether by omission or by the violation of the applicable legal rules or the provisions hereof, shall be liable for the damage caused.

7. MISCELLANEOUS PROVISIONS

- 7.1. This Data Processing General Terms and Conditions shall take effect on the date set out and continue to be in force until the termination of the Master Contract. Should this Data Processing General Terms and Conditions be terminated, the Parties shall review whether they are obliged to delete, destroy or in accordance with the GDPR and/or other legislation further process is possible to be the continued of such data. The liability related to such continued processing of the personal data shall rest solely with the Party performing such processing.
- 7.2. In the course of their cooperation under this Data Processing General Terms and Conditions, the Parties shall mutually appoint their respective contact persons. Any questions or declarations to be raised or made in connection with the performance of this Data Processing General Terms and Conditions shall be dealt with by the Parties through their designated contact persons. Any declaration made through a different channel shall have a legal effect subject to the consent of the Party concerned.

The Parties shall process the personal data provided in this Data Processing General Terms and Conditions for the purpose of keeping contacts with the other Party and the performance of the rights and obligations hereunder, in the legitimate interest of the Parties, and retain such data for 8 years. The Parties represent that they have fully informed the data subjects of the processing of their personal data, as well as their rights related thereto, and that they are duly authorized to transfer such personal data to the other Party.

- 7.3. This Joint Controller Agreement shall be governed by the laws of the Parties and the European Union. Matters not regulated herein shall be governed in particular by the provisions of the GDPR, the Hungarian Civil Code and Act CXII of 2011 ("Privacy Act").
- 7.4. The Parties agree to strive at settling any disputes arising herefrom amicably. Should such attempts of the Parties fail, they agree to submit to the jurisdiction of the Hungarian courts of law.
- 7.5. This Data Processing General Terms and Conditions may only be amended by the Parties in writing.

Appendix 1

A) The subject matter of processing: data transfer under the student exchange program.

B) Nature and purpose of the processing: Participation of students in the student exchange program the enforcement of claims related to the student exchange program

C) Duration of data processing: In the case of data necessary for the performance of the agreement on the student exchange program and the data necessary for the enforcement of claims related to the student exchange program: 60 days from the termination of the agreement on the student exchange program.

D) Categories of persons concerned: University students.

E) Types of personal data processed:

1. name of the data subject
2. mother's maiden name
3. gender
4. place and date of birth
5. native language
6. citizenship
7. passport or ID card number
8. home address
9. temporary residence in the host country
10. emergency contact (name, phone, address, email address) (data subject is liable for obtaining the consent of the contact person before providing his, her data to the data processors)
11. first email address
12. second email address
13. mobile phone number
14. level of studies
15. field of studies
16. transcript of records
17. level / scores of language exam
18. copy of language exam certificate
19. copy of bachelor degree or secondary school certificate
20. position

The above data set covers all personal data that can be processed, but depending on the student exchange program may not all of these data will be processed. Upon request of the data subject, the Data Controllers inform him/her on the specific data processed related to him/her.

F) Technical and organizational measures related to the activities of the Data Controllers:

- (i) preventing unauthorized access to systems that also process personal data;
- (ii) ensuring that persons having access to data processing systems have access only to data appropriate to their respective levels of authorization and that personal data cannot be read, copied, altered or erased by unauthorized persons during their collection or use or after their recording;
- (iii) ensuring that personal data cannot be read, copied, altered or erased by unauthorized persons during electronic transmission, transfer or recording on a storage medium and that it is possible to

verify or identify where the personal data was transmitted by means of the data transmission equipment;

(iv) ensuring that it is possible to retrospectively determine by whom and when the personal data was entered, altered or erased into/from the Processing System(s);

(v) ensuring that personal data processed by subcontractors can only be processed in accordance with the instructions of the client;

(vi) ensuring that the personal data is protected against unintentional destruction or loss;

(vii) ensuring that personal data is protected against accidental or unlawful alteration or unauthorized disclosure.