# PRIVACY ADDENDUM

# Exchange of personal data between controllers

This Privacy Addendum (“Addendum”) is made and entered into on [insert date] (“Effective Date”) by and between [insert name of university], a university located in [insert country], and [insert name of university], a university located in [insert country], collectively referred to as the “Parties” or individually as a “Party”.

WHEREAS, the Parties wish to enter into an agreement for the Processing of Personal Data in accordance with the 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 (“GDPR”) Article 46(2)(a) for the purpose of Processing Personal Data when sending exchange students between the two universities.

THEREFORE, The Parties have agreed on the following contractual clauses as the legally binding instrument between the parties for transfer of Personal Data:

**For University [insert name] acting as an independent Controller when transferring Personal Data under this agreement.**

Name: ……………………………………  
  
  
Sign: ………………………………………

**For University [insert name] acting as an independent Controller when receiving Personal Data under this agreement.**

Name: ……………………………………  
  
  
Sign: ………………………………………

Date [dd/mm/year]:

# Definitions

For the purposes of this Agreement, the following terms shall have the meanings set forth below:

(a) “Controller” means both parties acting as independent controllers who have agreed on the purposes and individually determine the means of the Processing of Personal Data.

(b) “The Transferring University” means the university which transfer the Personal Data under the Addendum as an independent Controller.

(c) “The Receiving University” means the university which imports the data under the Addendum as an independent Controller.

(d) “Personal Data” means any information relating to an identified or identifiable natural person (the data subject), as defined in the GDPR.

(e) “Processing” means any operation or set of operations which is performed on 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.

(f) "Sensitive data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person (the data subject), health data, or data concerning a natural person's (the data subject) sex life or sexual orientation.

(g) “Addendum” means this specific document named as addendum.

(h) “Agreement" means the co-operation agreement “[insert name of main Agreement]” entered into by the Parties on [Insert date]

# Purpose, description and Duration of Processing

2.1 The purpose of the Processing of Personal Data under the Agreement and this Addendum is to facilitate the exchange of students between the Parties.

2.2. The transfer of Personal Data set out in section 3.2 is made from the Transferring University to the Receiving University after confirmation of exchange of the student in the accordance with the Agreement. The transfer will entitle the Receiving University to make contact with the student enrolled in the exchange program. Under this Addendum both parties individually commit to ensuring an adequate level of protection as granted under the GDPR as individual controllers.

2.2 The duration of the Processing of Personal Data under the Agreement and this Addendum shall be for the duration of the Agreement.

# Categories of Personal Data and data subjects

3.1 The following categories of data subjects may be processed in accordance with this Addendum:

* Students
* Contact persons and other employees at the Parties

3.2 The following categories of Personal Data can be processed by the Parties in accordance with this Addendum:

Registered subjects: The students

* Name and contact information of exchange student.
* [other categories of personal must be included when applicable]

Registered subjects: Contact persons and other relevant employees at the Parties.

* Name and contact information of contact person and other relevant employees of the Parties.

No special category is processed under this Addendum.

3.3 The Receiving University shall not process any other Personal Data occasionally received from the Transferring University, without the prior specific written consent of the Transferring University.

# Obligations of the transferring university

4.1 The Transferring University shall ensure that it has one of the legal bases set forth in Article 6 of the GDPR, as required by the GDPR for the Processing and transfer of Personal Data.

4.2 The Transferring University shall provide the Receiving University with all necessary information regarding the Processing of Personal Data under this Addendum.

# Obligations of the REceiving University

5.1 The Receiving University shall process Personal Data only in accordance with the specific purpose(s) of the transfer, as set out in section 2 and in compliance with the GDPR and all other laws and regulations included in the governing law of the Addendum.

5.2 The Receiving University shall only process Personal Data stated in section 3. If the Receiving University receives or becomes aware of processing of categories of personal data not stated in section 3, the Receiving University must delete this Personal Data and notify the Transferring University without undue delay.

5.2 The Receiving University shall ensure that all employees and other persons who have access to Personal Data under this Addendum are bound by appropriate confidentiality and data protection obligations.

5.3 The Receiving University shall take appropriate technical and organizational measures to ensure the security of Personal Data and to prevent unauthorized access, use, alteration, or destruction of Personal Data, and as a minimum take all measures required pursuant to art. 32 in GDPR.

5.4 The Receiving University shall assist the Transferring University in ensuring compliance with the obligations pursuant to art. 32 and 36 taking into account the nature of Processing and the information available to the Receiving University.

5.5 The Receiving University shall promptly notify the Transferring University of any unauthorized access, use, alteration, or destruction of Personal Data.

# Data Protection Principles

6.1 The Parties will ensure that the core data protection principles in GDPR are ensured. All Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

6.2 Any further Processing of Personal Data shall only occur with the explicit consent of the data subject directly to the Receiving University or in cases where such further Processing is necessary for a lawful purpose compatible with the original purpose of the transfer, as permitted by GDPR and protection laws and regulations include in the governing law of this Addendum. The Parties shall ensure that Personal Data is not further processed in a manner that is incompatible with the purpose of the Agreement and this Addendum. Any further Processing of Personal Data by the Receiving University shall be notified to the Transferring University before such further Processing takes place and the Transferring University may then oppose for specific reasons.

6.3 The Parties agree to ensure that Personal Data transferred under this Addendum is accurate, complete, and up-to-date. To this end, the Parties shall take appropriate measures to ensure that Personal Data is rectified, erased, or supplemented without delay where it is inaccurate or incomplete. If one of the Parties becomes aware that inaccurate or out of date data has been transferred or is being Processed, it must notify the other Party without delay.

6.4 The Parties shall also ensure that Personal Data is not retained for longer than necessary for the purposes for which it was transferred or as required by applicable laws and regulations.

# Security and Confidentiality of Personal Data

7.1 The Parties shall commit to ensuring the security and confidentiality as well of the Personal Data Processing and transfers they carry out.

7.2 The Parties shall have in place appropriate technical and organizational measures to protect Personal Data against accidental or unlawful access, destruction, loss, alteration, or unauthorized disclosure. These measures shall include, for example, encryption in transit and at rest, restricting who has access to Personal Data, providing secure storage of Personal Data, and implementing policies designed to ensure Personal Data are kept secure and confidential.

7.3 The level of security measures shall take into consideration the risks, the state of the art, and the related costs.

7.4 The Parties shall notify each other without undue delay and no later than 48 hours after becoming aware of any Personal Data breach. The notification shall include details of the breach, the categories of Personal Data affected, and the measures taken to address the breach.

7.5 The Parties shall take reasonable and appropriate measures to remedy any Personal Data breach and minimize the potential adverse effects, including by communicating to the data subject a Personal Data breach, without undue delay, where that Personal Data breach is likely to result in a high risk to the rights and freedoms of the natural person.

7.6 The Receiving University shall promptly notify the Transferring University in the event of any breach of security or confidentiality that affects Personal Data processed under this Addendum, and shall cooperate with the Transferring University to investigate and remediate any such breach. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the Receiving University shall without undue delay notify both the Transferring University and the competent supervisory authority. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Receiving University to provide all the information at the same time, it may do so in phases without undue further delay.

7.7 In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the Receiving University shall also notify without undue delay the data subjects concerned of the Personal Data breach and its nature, if necessary in cooperation with the Transferring University, together with the information referred to in section 7.6 points ii) to iv), unless Receiving University has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts.

7.8 The Parties shall ensure that their respective personnel who have access to the Personal Data are trained on the appropriate handling and protection of Personal Data and comply with the GDPR and all other laws and regulations in the governing law of the Agreement and this Addendum.

# Right to Transparency

8.1 The Parties shall ensure transparency in the Processing of Personal Data pursuant to this Agreement.

8.2 The Transferring University shall ensure that individual information to data subjects is made by the Transferring University in accordance with the notification requirements of Articles 13 and 14 GDPR. A general information notice on the website of the Transferring University is not sufficient. The Transferring University shall provide the data subject with clear and concise information about the Processing of Personal Data, including but not limited to the following:

i. The identity and contact details of the Transferring University, and any third-party data processors involved in the Processing;

ii. The purposes and legal basis for the Processing;

iii. The categories of Personal Data processed;

iv. The recipients or categories of recipients of the Personal Data;

v. The retention period for the Personal Data;

vi. The data subject’s rights under GDPR, including the right to access, rectify, erase, and restrict Processing of their Personal Data;

vii. The right to lodge a complaint with a supervisory authority and the available redress mechanism.

The Receiving University shall publish the information stated in i. -vii. on their website.

8.3 The Parties shall commit to making the Addendum available to data subjects on request and to make the Addendum or the relevant provisions providing for appropriate safeguards publicly available on their website.

8.4 The Parties shall ensure that their respective personnel who are responsible for Processing and transferring Personal Data are adequately trained on transparency obligations and comply with the GDPR and all other applicable laws and regulations in the governing law of this Addendum.

# Documentation and compliance

9.1 Each Party shall be able to demonstrate compliance with its obligations under this Addendum. In particular, the Receiving University shall keep appropriate documentation of the processing activities carried out under its responsibility.

9.2 The Receiving University shall make such documentation available to the competent supervisory authority on request.

# Subprocessing

10.1 The Receiving University shall not subcontract any of its obligations under this Addendum without the prior written consent of the Transferring University.

10.2 If the Receiving University subcontracts any of its obligations under this Addendum, it shall ensure that the subcontractor is bound by the same data protection obligations as the Receiving University under this Addendum.

10.3 Where the Receiving University engages a sub-processor to carry out specific processing activities (on behalf of the Receiving University), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under this Addendum.

10.4 The Receiving University shall remain fully responsible to the Transferring University for the performance of the sub-processor’s obligations under its contract with the Receiving University. The Receiving University shall notify the Transferring University of any failure by the subprocessor to fulfil its obligations under that contract.

# Return or Deletion of Personal Data

11.1 Upon the termination of this Addendum or upon the Transferring University’s request, the Receiving University shall return or delete all Personal Data processed received from the Transferring University under this Addendum, unless the retention of such data is required by law.

11.2 Personal Data is to be deleted by either Party when the information has been processed unlawfully or is no longer necessary for the purpose of Processing.

# Miscellaneous

12.1 This Addendum constitutes the entire agreement between the Parties with respect to the processing of transferred Personal Data hereof and supersedes all prior or contemporaneous agreements or understandings, whether written or oral with respect to the processing.

12.2 This Addendum may not be amended or modified except in writing.

# Rights of Data Subjects

13.1 The Parties shall ensure that data subjects have the right to exercise their rights under the GDPR, including the right to access, rectify, erase, restrict Processing, object to Processing, and data portability.

13.2 The Parties shall promptly notify each other if they receive a request from a data subject under the GDPR, and shall provide all necessary assistance to the other Party to enable it to respond to such request. The Receiving University, where relevant with the assistance of the Transferring University, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her Personal Data and the exercise of his/her rights under this Addendum without undue delay and at the latest within one month of the receipt of the enquiry or request.

# Restrictions on Onward Transfers and Sharing of Data

14.1 Onward transfers of Personal Data by the Receiving University to recipients not bound by this Addendum shall be specifically excluded, unless such transfers are necessary to achieve the purpose specified in clause 2 above and are permitted by data protection laws and regulations in the law governing this Addendum. Any such transfers shall be subject to prior and express authorization by the Transferring University and shall be accompanied by appropriate safeguards to ensure that the level of protection afforded to Personal Data is not diminished. These safeguards shall include a commitment by the receiving third parties to respect the same data protection principles and safeguards as included in this Addendum, including providing data subjects with the same data protection rights and guarantees. The Parties shall ensure that any onward transfers are consistent with the purpose limitation principle in GDPR and shall take appropriate measures to ensure that Personal Data is not processed beyond what is necessary for the purposes specified in clause 2 above.

14.2 If the Receiving University receives a request for onward transfer of Personal Data from a third party, it shall promptly notify the Transferring University and seek its prior written consent before proceeding with such transfer.

14.3 Disclosure or government access to Personal Data shall only be permitted to the extent required by applicable law, regulation, or court order. In any case, any disclosure of Personal Data to other third parties or public authorities is only permitted when it’s necessary and proportionate in a democratic society to safeguard important objectives of public interest in line with the ones listed in Article 23 (1) GDPR. The Parties shall inform each other as soon as possible if they receive a request for disclosure or government access to Personal Data, unless prohibited by applicable law. The Parties shall take all reasonable steps to challenge any such requests that are not legally valid or are overbroad in scope, and to protect the privacy rights of data subjects.

# Redress Mechanism

15.1 Data subjects are able to complain to each of the Parties for non-compliance with the data protection safeguards outlined in this Addendum, independently of who of the parties that have caused the non-compliance.

15.2 The Parties is required to establish effective routines to handle and resolve complaints from data subjects in a timely manner. This also provides the data subjects with the possibility of obtaining administrative redress from the independent data protection authority in the jurisdiction of the governing law of this Addendum. The Parties shall cooperate in good faith to resolve any such complaints or concerns.

15.3 Both Parties will be liable for compensation of damages resulting out of the Processing of Personal Data being not in compliance with GDPR and law or regulation in the governing law of this Addendum, regardless of which of the Parties that has caused the non-compliance.

15.4 The Parties must inform each other of the outcome of any proceedings, especially if a complaint is dismissed or not resolved.

15.5 The Transferring University may suspend or terminate the transfer of Personal Data under the Addendum if the Parties are unable to resolve a dispute amicably until the issue has been satisfactorily addressed by the Receiving University. If such a suspension or termination occurs, the Receiving University must commit to returning or deleting the Personal Data.

# Supervision Mechanism

16.1 Both Parties acknowledge and agree that in order to ensure compliance with this Addendum, it is necessary to establish appropriate independent supervision mechanisms to monitor the proper application of the Addendum and to prevent any interference with the rights provided under the Addendum.

16.2 Each Party confirm that they conduct periodic internal checks to ensure compliance with the Addendum and the effective application of the safeguards provided herein. The results of such checks shall on request be communicated to the other Party and, if applicable, to the independent data protection authority in the jurisdiction of the governing law of this Addendum. Each Party may request an audit by an independent auditor to confirm that the other Party ensures compliance with this Addendum. The Party requesting the independent audit shall bear all costs in relation to the independent audit.

16.3 Each Party shall inform the other Party without delay if it is unable to effectively implement the safeguards provided in this Addendum for any reason. In such cases, the Transferring University may suspend or terminate the transfer of Personal Data to the Receiving University until such time as the Receiving University informs the Transferring University that it is able to act consistently with the safeguards provided in this Addendum.

16.4 Each Party shall cooperate with the competent supervisory authority in the jurisdiction of the governing law in this Addendum, including providing all necessary information and assistance, to enable the other Party to comply with its obligations under the GDPR.

16.5 Each Party shall promptly notify the other Party of any communication from a competent supervisory authority in the jurisdiction of the governing law, regarding the Processing of Personal Data under this Addendum.

# Automated individual decision-making

The Receiving University shall not make any decision solely based on automated individual decision-making, including profiling, which produces legal effects concerning the data subject in question or similarly affects this data subject.

# Point of contact regarding the processing of personal data

The Parties shall each designate a person in their organizations to receive the relevant Personal Data as well as to respond to inquiries regarding the Processing of Personal Data;

for [Name of institution]

Mr/Mrs. xx, (Department)

For [Name of institution]

Mr/Mrs. xx, (Department)

# Termination

19.1 Either Party may terminate this Addendum upon written notice to the other Party if the other Party breaches any material provision of this Addendum and fails to remedy such breach within thirty (30) days after receipt of written notice of such breach.

19.2 Upon termination of this Addendum, the Receiving University shall return or delete all Personal Data processed under this Addendum, unless the retention of such data is required by law.

# Competent supervisory authority

The Parties agree that the Norwegian Data Protection Authority (Datatilsynet) is the competent supervisory authority under this Addendum.

# Liability

Each of the Parties may claim:

* compensation for loss and expenses; and
* demand recourse of alle claims and administrative fines

from the other Party to the extent such loss, expenses, claims or administrative fines are based on that the other Party has not been in compliance with its obligations under this Addendum.

Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under this Addendum. This is without prejudice to the liability of the Transferring University under Regulation (EU) 2016/679.

# Venue and governing law

This Addendum shall be governed by and every reference to law or regulation in this Addendum shall be to, Norwegian Law. Any dispute concerning this Addendum shall be settled by ordinary courts in Norway.

**In witness whereof, each of the Parties hereto has caused this Addendum to be executed by its duly authorised officers or representatives.**

**For Transferring University:** **For Receiving University:**

Name: Name:

Address: Address:

Date: Date:

Role: Controller Role: Controller

Sign: Sign: