AGREEMENT BETWEEN DATA PROCESSOR AND SUB-PROCESSOR ON PROCESSING PERSONAL DATA

(SUB-PROCESSOR AGREEMENT)

According to applicable Norwegian personal data legislation and EUs General Data Protection Regulation 2016/679 of 27 April 2016 ("GDPR"), (especially article 28 nr. 4, cf. nr. 3), the following data processor agreement is made:

[Sub-title related to the specific project/conditions]

(«Agreement»)

between

***Name of institution/company*]**

[*org.no.*]

("Data Processor")

and

***Name of institution/company*]**

[*org.no.*]

("Sub-processor")

IMPORTANT NOTE ON THE USE OF THIS TEMPLATE:

Note that the individual sub-processor agreement to serve its purpose must be a direct reflection of similar provisions in the main data processor agreement between the controller and the data processor. This template is based on the fact that UiO's standard template for (main) data processor agreement is used between the controller and the data processor. In all cases, regardless of the contract template used for the main data processor agreement, it is important that all provisions of the sub-processor agreement are quality assured carefully against all provisions of the master data processor agreement to verify that each provision is properly mirrored from the data processor to the sub-processor, cf. GDPR Article 28 (4)]

Text in italics should be removed and replaced with relevant text, or with one of several alternatives where applicable.

1. Purpose of the Agreement

The purpose of the Agreement is to regulate rights and obligations in relation to the applicable Norwegian personal data legislation and EUs General Data Protection Regulation 2016/679 of 27 April 2016 ("GDPR").

The Agreement governs the processing of personal data by sub-processors on behalf of data processors, including the collection, registration, compilation, storage or disclosure of personal data, or combinations thereof, in connection with *[name of project]* in accordance with agreement between the parties entered into *[date]* ("Main Agreement").

Sub-processor understands that the Data Processor acts on behalf of a Data Controller for the personal data covered by the agreement, and that Sub-processor are subject to similar obligations as the Data Processor is required by the Data Controller in accordance with Article 28 (4) GDPR.

The agreement shall ensure that personal data is not used illegally, unlawfully or that the information is processed in ways that lead to unauthorized access, alteration, deletion, damage, loss or inaccessibility.

In the event of a conflict, the terms of this agreement shall precede the privacy statement of the Sub-processor or the terms of other agreements entered into between the Data Processor and the Sub-processor in connection with the main agreement.

It must be stated in Annex 1 to the agreement if the Sub-processor can use its own sub-contractors under the Agreement, including for storage, processing or other use, cf. clause 8.

The purpose of the processing, the types of processing activities, categories of data subjects and the types of personal data that will be processed are set out in Annex 1 of the Agreement. These conditions cannot be changed by either party without a new agreement or an amendment to the agreement being signed.

2. Instructions

Sub-processors shall follow the written and documented instructions for the processing of personal data that the Data Processor has decided to apply.

Sub-data processors undertake to comply with all obligations in accordance with the applicable Norwegian personal data law applicable to the processing of personal data.

Sub-processor undertakes to notify Data Processor if Sub-processor receives instructions from Data Processor that violates the privacy regulations.

> *Note: Detailed instructions for Sub-processor can be attached as an appendix to the Agreement.*

3. The rights of registered subjects

The Sub-processor is obliged to assist the Data Processor in the treatment of the data subject's compliance with the data subject's rights in accordance with current Norwegian personal data legislation.

The data subject's rights include the right to information on how his or her personal data is processed, the right to demand access to his own personal data, the right to demand rectification or deletion of his personal data and the right to demand the processing of his personal data.

To the extent applicable, the Sub-processor shall assist the Data Processor in connection with the Data Controller's protection of data subjects' right to data portability and the right to oppose automatic decisions, including profiling.

Sub-processor is liable to the data subject if errors or negligence of Sub-processor incurs the recorded financial or non-financial losses due to their rights or privacy being violated.

4. Satisfactory information security

Sub-processor shall ensure appropriate technical, physical and organizational security measures to protect personal data covered by this Agreement against unauthorized or unlawful access, alteration, deletion, damage, loss or inaccessibility.

Sub-processor must document their own security organization, guidelines and procedures for security work, risk assessments and established technical, physical or organizational security measures. The documentation should be available to the data processor. Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

Sub-processor will establish continuity and contingency plans for effective management of serious security incidents. The documentation should be available to the Data Processor. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

Sub-processor shall provide sufficient information and training to their own employees in order to safeguard the security of personal data processed on behalf of the Data Processor.

Sub-processor must document the training of their own employees in information security. The documentation should be available to the Data Processor. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

> *Note: It may be necessary to specify the most important security measures implemented by the Sub-processor, possibly referring to documents or publications explaining how the Sub-processor works with information security and the security measures established for the service in question. The concretizations can be included in the Agreement itself or in annex to the Agreement.*

5. Confidentiality

Only employees of Sub-processor who have a service need for access to personal data managed on behalf of a Data Processor can be granted such access. The Sub-processor is required to document access control policies and procedures. The documentation should be available to the Data Processor. The Data Processor can provide the Data Controller with

access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

Sub-Processors shall ensure that employees of Sub-Processors are subject to a duty of confidentiality regarding documentation and personal data that they may have access to in accordance with this Agreement. This provision also applies after termination of the agreement.

Norwegian law may limit the scope of the duty of confidentiality for employees of sub-processors and sub-contractors.

6. Access to documentation

The Sub-processor is obliged to provide the Data Processor with access to all documentation that is necessary for the Data Processor to assist Data Controller to fulfill his/her duties under the current Norwegian personal data legislation.

Sub-Processor is obliged to provide the Data Processor with access to other relevant documentation that enables the Data Processor to assess whether the Sub-processor complies with the terms of this Agreement.

The Data Processor may provide the Data Controller with access to the documentation to enable the controller to fulfill his/her obligations under the applicable Norwegian personal data legislation, but also has a duty of confidentiality with regard to confidential documentation that the Sub-processor makes available to the Data Processor.

7. Duty to notify in case of security breach

Sub-processor shall notify the Data Processor without undue delay if personal data processed on behalf of the Data Processor is exposed to security breaches which entail a risk of violations of the data subjects' privacy.

The notification to the Data Processor shall include, as a minimum, information describing the breach, which data subjects are affected by the breach, what personal information is affected by the breach, what immediate action has been taken to deal with the breach, and any preventive measures that may have been taken to avoid it similar events in the future.

The Data Processor is responsible for ensuring that notifications of security breaches from the Sub-processor are passed on to the Data Controller.

8. Subcontractors

Sub-processor is obliged to enter into separate agreements with any subcontractors that regulate the subcontractor's processing of personal data on behalf of Sub-processor.

In agreements between Sub-processor and subcontractors, subcontractors shall be required to fulfill all obligations that the Sub-processor itself is subject to under this Agreement. The sub-processor is required to submit the agreements to Data processor on request. The Data Processor may submit the agreements to the Data Controller.

Sub-processor shall verify that all subcontractors comply with their contractual obligations, in particular that information security is satisfactory and that subcontractor employees are aware of their obligations and fulfill them.

Data Processor approves that the Sub-processor engages the subcontractors listed in Appendix 1 to this Agreement.

Sub-processor cannot engage subcontractors other than those listed in Appendix 1 without prior approval of the Data Processor. In the event of such a change, an amendment document must be attached as an annex to this Agreement, dated and signed by both parties.

Sub-processor is liable for damages in accordance with Clause 13 for financial losses of the Data Processor due to illegal or unlawful processing of personal data or insufficient information security of subcontractors.

9. Transfer to countries outside the EU/EEA

Note: Personal data processed by a sub-processor on behalf of a data processor may be transferred to countries outside the EU / EEA (third countries). Such transfer may occur under certain conditions. The rules on transfer to third countries can be found in Articles 45-47 and 49 of the EU's Privacy Regulation. The rules also apply to backup and other transfer of personal data that occurs in connection with the administration of the service in question, such as support. These rules mean, among other things, that the transfer will be legal if it happens to an EU-approved third country, to US companies in the United States that have joined the Privacy Shield scheme for the type of information provided in that particular company's affiliation, or on the basis of EU standard contracts for the transfer of personal data to third-country data processors (EU's "Standard Contractual Clauses"). Use of the latter requires the agreement to be entered into directly between the controller and the sub-processor, which is often arranged by a contract authorization from the controller to the data processor. A privacy lawyer should be conferred in these cases.

Include if relevant:

Personal data processed under this Agreement will be transferred to, or accessed from, the following recipient countries outside the EU/EEA:

……...
(recipient country name)

The legal basis for the transfer of personal data to the said recipient countries outside the EU/EEA is:

……...
(brief explanation of the transfer basis)

10. Security audits and impact assessments

Sub-processors shall regularly carry out security audits of their own work to secure personal data against unauthorized or illegal access, alteration, deletion, damage, loss or unavailability.

Sub-processors will conduct security audits of the information security in the business. Security audits shall include the Sub-processor's security objectives and security strategy, security organization, guidelines and procedures for security work, established technical, physical and organizational security measures and work on information security with subcontractors. It shall also include procedures for alerting Data Processor in case of security breaches and routines for testing contingency and continuity plans.

Sub-processors must document the security audits. The Data Processor shall be given access to the audit reports. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

If an independent third party conducts security audits at the Sub-processor, the Data Processor shall be informed of which auditor is used and have access to summaries of the audit reports. The Data Processor can provide the Data Controller with access to summaries of the audit reports in order for the Data Controller to fulfill his/her duties according to current Norwegian personal data legislation.

> *Note: The parties can agree that the Data Processor itself performs security audits at the Sub-processor, possibly also how costs incurred in connection with such audits should be distributed. This can be included here, possibly in the service agreement.*

Sub-processors shall, at the request of the Data Processor, assist the Data Processor if the use of the service means that the Data Controller has an obligation to assess the consequences of privacy, cf. Regulation (EU) 2016/679, Articles 35 and 36. Sub-processor can assist in the implementation of privacy-promoting measures if the impact assessment shows that this is necessary.

11. Return and deletion

Upon termination of this Agreement, the Sub-processor is obliged to delete and/or return all personal data processed by the Sub-processor on behalf of the Data Processor in connection with the Main Agreement. The Data Processor decides how the return of personal data should take place, including the format to be used.

Sub-processors shall delete personal data from all storage media containing personal data processed by the Sub-processor on behalf of the Data Processor. Deletion must occur by sub-processor using a deletion tool approved by the Data Processor or by overwriting. This also applies to backups of personal data.

Sub-processors shall document that deletion of personal data has been carried out in accordance with this Agreement. The documentation shall be made available to the Data Processor. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Norwegian personal data legislation.

Sub-processor covers all costs associated with the return and deletion of the personal data covered by this Agreement.

Note: The parties may agree further on how the costs incurred in connection with the deletion or return of personal data shall be allocated, either in this Agreement or in the Main Agreement.

12. Breach

In the event of any material breach of the terms of this Agreement due to errors or negligence on the part of the Sub-processor, the Data Processor may terminate the Agreement with immediate effect. Sub-processors will continue to be obliged to return and/or delete personal data processed on behalf of the Data Processor in accordance with the provisions of clause11 above.

13. Compensation

The Data Processor may claim compensation for financial losses that errors or neglect on the part of the Sub-processor, including breach of the terms of this agreement, have caused the Data Processor, cf. also paragraphs 3 and 8 above.

[The following paragraphs are included if UiO is the Sub-processor]:

Sub-processor is liable for direct financial loss, including administrative infringement fees and claims that are addressed to the Data Processor, which can be reversed in violation of the Sub-processor's obligations under this agreement.

Total compensation per calendar year is limited to an amount equal to the total annual remuneration of the Main Contract, excl. VAT.

If a sub-processor or someone the sub-processor is responsible for has acted with gross negligence or willful intent, the aforementioned compensation limitations do not apply.

14. The Agreements duration

This Agreement applies as long as Sub-processor processes personal data on behalf of Data Processor originating in the Main agreement.

15. Contacts

The contact at Data Processor for questions related to this Agreement is: _____.

[Unit, position, contact information, address, telephone and email]

The contact at Sub-processor for questions related to this Agreement is: _____.

[Unit, position, contact information, address, telephone and email]

16. Choice of Law and Venue

Note: Choose the appropriate option depending on the contracting party:

Option 1 - applies when UiO's counterparty is a private entrant/non-governmental university or college:

The agreement is governed by Norwegian law. The parties adopt *[enter name of district court]* as venue.

Option 2 - applies when UiO's counterparty is another state university or college.

The agreement is governed by Norwegian law. Any disputes arising out of this Agreement shall first be tried resolved through negotiation. If the parties do not reach agreement through negotiations, the dispute shall be resolved with binding effect by the *Ministry of Education/Oslo District Court*. Either party may request that the dispute be forwarded to the *Ministry/District Court.*

***

This Agreement is in 2 – two – copies, each of the parties retain their own copy.

Place and date

……..

On behalf of [Data Processor]	On behalf of [Sub-processor]
……..	……
(Signature)	(Signature)

ANNEX 1 – SPECIFICATION OF THE DATA PROCESSING

1. Purpose

The purpose of the parties' processing of personal data under the Agreement is:

Note: Clearly state what the parties' purpose of the data processing is. If the purpose is stated in another agreement between the parties, it may be referred to.

2. Types of personal data

The following types of personal data will be processed by the parties under the Agreement:

Note: Give a brief (preferably point by point) overview of the main types of personal data that will be processed by the parties. Indicate whether they are sensitive and whether the data is directly identifiable or unidentified (ie. if the data appears anonymous, but where one can actually go back and find out who the data/information applies to).

3. Categories of registrered subjects/data subjects

The personal data processed under the Agreement relate to the following categories of data subjects:

Note: Give a brief overview of who the information applies to, such as students and staff at the institution.

4. Description of roles

Data Processor will mainly have the following role and perform the following processing activities under the Agreement:

Note: Provide an overall description of the party's role in relation to data processing and the main types of processing activities he or she will perform.

Sub-processor will mainly have the following role and perform the following processing activities under the Agreement:

Note: Provide an overall description of the party's role in relation to data processing and the main types of processing activities he or she will perform.

5. Approved subcontractors

The parties have agreed that the following subcontractors may be used by the respective parties under the Agreement:

Data Processors subcontractors:

[Specification of any authorized subcontractors.]

Sub-processors subcontractors:

[Specification of any authorized subcontractors.]