

## Agreement on joint controllership

between

OsloMet - Storbyuniversitetet

Org. no.: 997 058 925

Post box 4, St. Olavs plass

0130 Oslo

Norway

(hereinafter referred to as «Controller 1»)

and

[Name of institution]

[Org. no.]

[Address]

(hereinafter referred to as «Controller 2»)

## Object of the agreement

The parties have entered into an agreement on project cooperation (the “Main Agreement”), which involves processing of personal data. For this processing, the parties will be considered joint controllers since the parties jointly determine the purposes and means of the processing.

This agreement (the «Agreement») establishes the parties’ respective responsibilities for compliance with the obligations under Regulation 2016/679/EU (the “GDPR”) and other applicable privacy legislation in relation to the processing of the personal data. This Agreement constitutes the arrangement required by and described in the GDPR article 26 and shall regulate the respective responsibilities of the parties with regards to the exercising of the rights of the data subjects and their respective duties to provide the information referred to in GDPR articles 13 and 14.

In the event of conflict, the terms of this Agreement will take precedence over the parties’ privacy policies and the terms of the Main Agreement entered into between the parties.

## Purpose and description of the joint processing activities

The purpose of the joint processing is to carry out the project cooperation as described in the Main Agreement. The parties shall not process the personal data for other purposes than the ones stated in this Agreement or to a greater extent than necessary to fulfil their obligations under the Main Agreement, unless otherwise prescribed by mandatory law. In such cases, the other party shall be informed of that legal requirement before processing, unless that law prohibits such information.

A more detailed description of the purpose of the joint processing, the types of personal data processed, the categories of data subjects, and the respective roles and responsibilities of the parties in relation to the joint processing is set out in Appendix 1. These specifications cannot be changed by any of the parties without a written change of this Agreement.

## Compliance with the GDPR and other applicable privacy legislation

By signing this Agreement, the parties confirm the following:

* The parties shall comply with all provisions in the GDPR and other applicable privacy legislation in relation to the processing of personal data under this Agreement, including, but not limited to, compliance with the principles relating to processing of personal data as set out in the GDPR article 5.
* The parties shall have a valid legal basis in accordance with the GDPR articles 6, 9, and 10 for the processing of personal data under this Agreement.
* The parties comply with the requirement to maintain a record of processing activities in GDPR article 30, including to maintain a record of the processing activities for which the parties are joint controllers and to keep each other informed of the content in their records.
* The parties shall keep each other informed about important circumstances affecting the joint processing and this Agreement, including circumstances that affects or are able to affect a party’s ability to process personal data in accordance with this Agreement or fulfil the requirements in the GDPR or other applicable privacy legislation.

## Duty of confidentiality

Both parties shall ensure that the personal data processed under this Agreement is made available only to the parties’ employees or other affiliated persons who have a documented need for such access to the personal data. Both parties shall also ensure that such employees or other persons who are authorised to process the personal data are subject to a duty of confidentiality with regards to documentation and personal data accessed under this Agreement. This provision also applies after the expiration of the Agreement. The duty of confidentiality includes the employees of third parties carrying out maintenance of (or similar tasks related to) systems, equipment, networks, or buildings used by the parties to carry out the project cooperation under the Main Agreement.

## Information security

Both parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in order to safeguard the personal data covered by this Agreement from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability, and take all measures required pursuant to GDPR article 32. The parties shall document the implemented technical and organisational measures.

As a minimum, the parties shall carry out risk assessments and implement measures to mitigate risks, establish continuity- and contingency plans for effective handling of serious security incidents, provide employees with information and training on information security, and on a regular basis carry out security audits of their own work on protection of personal data and of the systems and other relevant tools used for processing of the personal data related to the project cooperation carried out under the Main Agreement. The parties shall document their work with information security. Both parties are also responsible for compliance with the provision on data protection by design and default set out in GDPR article 25.

## The rights of the data subjects

Both parties are responsible for ensuring the data subjects’ rights in accordance with the GDPR Chapter III and other applicable privacy legislation. If a party receives a request from a data subject which is covered by the other party’s responsibilities, the request shall be forwarded to the other party as soon as possible. The parties shall assist each other to the extent relevant and necessary in order for both parties to be able to fulfil their obligations to respond to requests for exercising the data subject’s rights.

Both parties shall ensure that the data subjects are provided with information about the processing of personal data in accordance with the GDPR articles 13 and 14.

With regard to the fulfilment of the information obligation, the parties shall also make the essence of this Agreement available to the data subjects. This includes as a minimum:

* Information on the existence of a joint controllership
* The identity of the joint controllers
* Information on the respective roles of each of the joint controllers in relation to the joint processing as described in Appendix 1
* Information on that fact that each of the joint controllers has an obligation to comply with the rights of the data subjects under the GDPR Chapter III
* The contact point for the data subjects as described in section 7 and Appendix 1

## Contact point for data subjects

The parties may designate a contact point for data subjects in Appendix 1. If such contact point is designated, the data subjects may reach out to this contact point with questions on exercising of their rights. The contact point will then forward the request to the party responsible for the relevant circumstances. Notwithstanding the above, both parties have an independent responsibility for ensuring that the data subject’s rights are complied with.

## Notification of data breach

If personal data subject to the joint controllership under this Agreement is exposed to a data breach, both parties are responsible for compliance with the GDPR articles 33 and 34 on notification of personal data breach to the supervisory authority and/or the data subjects. The parties shall agree on which of them is responsible to fulfil the notification obligations on a case-to-case basis.

Both parties shall without undue delay notify the other party if personal data processed under this Agreement is exposed to a data breach. The notification shall as a minimum include information describing the security breach, which data subjects are affected by the breach, what personal data is affected by the breach, what immediate measures are implemented to address the breach, and what preventive measures have been established to avoid similar incidents in the future.

## Impact assessments

Both parties are responsible for carrying out a data protection impact assessment if required by GDPR article 35. Both parties are similarly responsible for complying with the requirement in the GDPR article 36 on prior consultations with the supervisory authority when necessary. The parties shall assist each other with the data protection impact assessments and the prior consultations with the supervisory authority. Both parties shall inform each other about the content and conclusion of a potential prior consultation.

## Information and audits

The parties shall, upon request, give the other party access to all information and documentation necessary to demonstrate compliance with the terms set out in this Agreement.

This information and documentation include, but is not limited to, documentation of security measures mentioned in section 5 (risk assessments and established security measures, continuity- and contingency plans for handling of serious security incidents, routines for information and training of employees, reports from own security audits security organisation, etc.), access documentation (guidelines and routines for access control), data processing agreements with sub-processors, legal basis for transfers to third countries, and other documentation necessary for the parties to meet its obligations under this Agreement, the GDPR, and other applicable privacy legislation

## Processors

The parties cannot use processors in relation to the joint processing of personal data unless this is approved in writing by the other party. The parties approve the use of the processors set out in Appendix 1. The parties cannot contract any other processors than those listed in Appendix 1 without prior written approval from the other party.

Each party is independently responsible for processors they contract and enter into an agreement with, even if the processor is used in connection with processing for which the parties are joint controllers under this Agreement. The responsible party for each of the approved processors is set out in Appendix 1.

This means that each of the parties are responsible for complying with the obligations set out in the GDPR article 28 in relation to their use of their own processors. The parties shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and other applicable privacy legislation. The parties shall also ensure that they enter into a valid data processing agreement with their processors and that this data processing agreement imposes on the processor all obligations necessary for the parties to fulfil their obligations towards each other under this Agreements. The parties shall ensure that their processors comply with the obligations imposed by the data processing agreement and the GDPR and other applicable privacy legislation.

This also means that to the extent a party suffer a financial loss, including administrative fines and claims for compensation, as a consequence of unlawful processing of personal data or insufficient information security on part of the other party’s processor, then this party shall remain fully liable to the other party.

## Transfers to countries outside the EU/EEA

The parties cannot transfer or allow transfer of personal data to countries or international organisations outside the EU/EEA or use processors in such third countries without prior written approval from the other party. This also includes remote access from third countries. In the event of such transfer to third countries or use of processors in third countries, the parties shall ensure that the provisions of the GDPR and other applicable privacy legislation are complied with, including that the transfer only takes place in accordance with the rules set out in the GDPR Chapter V.

An overview of the third countries to which the personal data processed under this Agreement will be transferred to and the legal basis for such transfers are set out in Appendix 1.

## Complaints

Each party have independent responsibility for considering potential complaints from the data subjects concerning breach of provisions of the GDPR and other applicable privacy legislation in connection with the processing of personal data that the party in question is responsible for under this Agreement.

The party receiving a complaint shall notify the other party as soon as possible if the complaint concerns the joint processing of personal data under this Agreement. The notification shall also state if, and if so to what extent, the party receiving the complaint will consider and respond to it. If one of the parties receive a complaint which should be considered in whole or in part by the other party, it shall forward the complaint to the other party as soon as possible. The data subject shall be informed about the essence of this agreement in connection with the party's forwarding of a complaint or part of a complaint to the other party.

## Breach and liability

If the parties do not fulfil their obligations under this Agreement or the GDPR or other applicable privacy legislation, it is considered a breach of this Agreement and the Main Agreement. In case of such breach, the parties may terminate the Main Agreement with immediate effect.

The parties can claim compensation for financial loss, including administrative fines and claims for compensation, suffered as a consequence of the other party’s breach of its obligations under this Agreement or the GDPR or other applicable privacy legislation. To the extent the financial loss is caused by unlawful processing of personal data or insufficient information security on part of a processor, the party responsible for that processor shall remain fully liable to the other party.

## Duration of the agreement

This Agreement applies for as long as the Main Agreement is in force, or as long as the parties process personal data as joint controllers.

## Contacts

The contact persons for the parties for questions and communications related to this Agreement are set out in Appendix 1.

## Choice of law, disputes, and legal venue

The parties’ rights and obligations under this Agreement are determined in full by Norwegian law. Any disputes arising out of this Agreement shall first be sought to be resolved through negotiations. If the parties do not reach agreement through negotiations, the dispute will be resolved with binding effect by Oslo District Court in Norway. If both parties are a state university or university college, the dispute will be resolved with binding effect by the Ministry of Education and Research. Either party may require that the dispute be sent to the Ministry.

\*\*\*

This Agreement is made in 2 – two copies, one for each party.

|  |  |
| --- | --- |
| Place and date: | Place and date: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  On behalf of Controller 1 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  On behalf of Controller 2 |
| Name: | Name: |
| Position: | Position: |

## Appendix 1

## Purpose(s) of the processing

[Description of the purpose(s) of the processing. This will as a general rule be to carry out the project cooperation in accordance with the Main Agreement. Give a summary of the cooperation to be carried out under the Main Agreement.]

## Categories of data subjects

[Describe the categories of data subjects of whom personal data is processed, such as employees, students, suppliers, etc.]

## Types of personal data

[Describe the types of personal data processed in relation to the data subjects, for example name, addresses, phone numbers, e-mails, etc. If relevant, please also indicate whether any special categories of data are processed, such as health data, ethnic origin, political opinions, etc.]

## Processing activities and the roles of the parties

Controller 1 has the following role and carries out the following processing activities under the Agreement: [Describe OsloMet’s role in relation to the joint processing activities, for example that OsloMet shall be responsible for the collection of the data for the project.]

Controller 2 has the following role and carries out the following processing activities under the Agreement: [Describe the other party’s role in relation to the joint processing activities, for example that they shall be responsible for the analysis of the collected data.]

## Processors within the EU/EEA

|  |  |  |
| --- | --- | --- |
| **Name** | **Processing activity** | **Responsible party** |
| [Analysis1] | [Analysis of data] | [Controller 2] |
|  |  |  |
|  |  |  |

## Processors outside the EU/EEA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Processing activity** | **Country** | **Legal basis for transfer** | **Responsible party** |
| [Microsoft Azure] | [Cloud provider] | [USA] | [Data Privacy Framework] | [Controller 1] |
|  |  |  |  |  |
|  |  |  |  |  |

## Contact point for data subjects

The parties have designated the following contact point for the data subjects: [Name, e-mail, phone]

## Contacts

Contact person for Controller 1: [Name, e-mail, phone]

Contact person for Controller 2: [Name, e-mail, phone]