****

## Data processing agreement

between

[Name of institution]

[Org. no.]

[Address]

(hereinafter referred to as the «Controller»)

and

[Name om service provider]

[Org. no.]

[Address]

(hereinafter referred to as «Processor»)

## 1. Object of the agreement

The parties have entered into an agreement on provision of services (the “Main Agreement”), which includes processing of personal data.

This data processing agreement (the “Data Processing Agreement”) regulates the parties’ rights and obligations when the Processor processes personal data on behalf of the Controller. The purpose of the Data Processing Agreement is to ensure that personal data is processed in accordance with Regulation 2016/679/EU (the “GDPR”) and other applicable privacy legislation.

In the event of conflict, the terms of this Data Processing Agreement will take precedence over the Processor’s privacy policy and the terms of the Main Agreement entered into between the Controller and the Processor.

## 2. Purpose limitation

The purpose of the Processor’s processing of personal data on behalf of the Controller is to deliver and administer the services described in the Main Agreement. A more detailed description of the purpose of the processing is set out in Appendix 1. The Processor cannot process the personal data for any other purpose without the prior written approval of the Controller.

## 3. Types of information and categories of data subjects

An overview of which types of personal data and which categories of data subjects the Processor processes on behalf of the Controller under this Data Processing Agreement is set out in in Appendix 1.

## 4. Instructions

The Processor shall only process the personal data in accordance with documented instructions from the Controller. Detailed instructions for the Processor are described in Appendix 1.

This also applies with regards to transfer of personal data to a third country or an international organisation, unless required by Union or Member State law to which the Processor is subject. In such cases, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Processor shall comply with all provisions in this Data Processing Agreement, in the GDPR, and other applicable privacy legislation.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable privacy legislation.

## 5. Confidentiality

The personal data processed on behalf of the Controller shall be made available only to the Processor’s employees or other affiliated persons who have a documented need for such access to the personal data.

The Processor shall 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 Data Processing Agreement. This provision also applies after the expiration of the Data Processing 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 Processor to provide or administer the services under the Main Agreement.

## 6. Information security

The Processor shall implement appropriate technical, physical and organisational safety measures to ensure a level of security appropriate to the risks, in order to safeguard the personal data covered by this Data Processing Agreement from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability. The Processor shall take all measures required pursuant to GDPR article 32 and assist the Controller in ensuring compliance with its obligations pursuant to this provision. Security measures are listed in the Appendix 1.

As a minimum, the Processor shall carry out risk assessments and establish measures to mitigate risks, establish continuity- and contingency plans for effective handling of serious security incidents and provide employees with information and training on information security. The Processor shall also 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 service provided under the Main Agreement.

## 7. The rights of the data subjects

The Processor shall, to the extent possible when taking into account the nature of the processing and by appropriate technical and organisational measures, assist the Controller with fulfilling the Controller's obligation to respond to requests for exercising the data subject's rights.

The rights of the data subjects include, but are not limited to, the right to information on how his or her personal data is processed, the right to request access to personal data, the right to request corrections to, or erasure of, their own personal data, and the right to require restriction of processing of their personal data.

To the extent relevant, the Processor will assist the Controller in maintaining the data subjects’ right to data portability and the right to object to automated decision-making, including profiling.

## 8. Notification of data breach

The Processor shall assist the Controller in ensuring compliance with its notification obligations pursuant to the GDPR articles 33 and 34.

If personal data processed on behalf of the Controller is exposed to a security breach which results in a risk to the rights and freedoms of the data subjects, the Processor shall notify the Controller without undue delay and within 36 hours at the latest by sending an e-mail to [sikkerhet@oslomet.no](mailto:sikkerhet@oslomet.no).

The notification to the Controller should, at minimum, include information that describes 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.

The Controller is responsible for ensuring that the Processor’s notifications of security breach are submitted to the Data Protection Authority and for notifying the data subjects if the Controller considers the security breach to result in a high risk to the rights and freedoms of the data subjects.

## 9. Impact assessments

The Processor shall assist the Controller in ensuring compliance with their obligations pursuant to GDPR articles 35 and 36. If the Controller considers it necessary to carry out a data protection impact assessment in accordance with GDPR article 35, the Processor shall assist the Controller with this assessment and the implementation of measures to ensure protection of personal data if the assessment shows that such measures are required. If the data protection impact assessment indicates that prior consultations with the Data Protection Authority are necessary in accordance with the GDPR article 36, the Processor shall assist the Controller with these consultations.

## 10. Information and audits

The Processor shall, upon request, give the Controller access to all information and documentation necessary to demonstrate compliance with the terms set out in this Data Processing Agreement.

This information and documentation include, but is not limited to, documentation of security measures mentioned in section 6 (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 Controller to meet its obligations under the GDPR and other applicable privacy legislation.

The employees of the Controller are subject to a duty of confidentiality in respect of confidential security documentation which the Processor makes available to the Controller.

The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller a third party on behalf of the Controller. When using a third party, such third party shall make a report to be provided to the Controller, which the Controller can make available to the Data Protection Authority or others who may have a need to know its content.

## 11. Sub-processors

If the Processor uses sub-processors, the Processor shall ensure that such sub-processors provide 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 Processor is also obliged to enter into separate agreements with sub-processors, imposing on them the same data protection obligations as set out in this Data Processing Agreement. The Processor shall ensure that sub-processors comply with the contractual obligations to which the Processor is subject under this Data Processing Agreement and other applicable privacy legislation.

All sub-processors shall be approved in writing by the Controller before the sub-processor can process personal data. The Controller approves the Processor’s use of the sub-processors set out in Appendix 1. The Processor cannot contract any other sub-processors than those listed in Appendix 1 without prior written approval from the Controller.

## 12. Transfers to countries outside the EU/EEA

Transfer of personal data to third countries or use of sub-processors in third countries is only allowed upon instructions from the Controller. This also includes remote access from third countries. In the event of such transfer to third countries or use of sub-processors in third countries, the Processor 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 Data Processing Agreement will be transferred to and the legal basis for such transfers are set out in Appendix 1.

## 13. Return and erasure

Upon termination of this Data Processing Agreement, the Processor is obliged to return and erase all personal data processed on behalf of the Controller in relation to provision of the services under the Main Agreement. The Controller determines how the return of the personal data will take place, including the format to be used.

The Processor shall cease the processing and erase the personal data from all storage media without undue delay after termination of the Data Processing Agreement, including back-up copies. Upon request from the Controller, the Processor shall provide a written statement that all personal data has been erased in accordance with this Data Processing Agreement. The Processor shall cover all costs related to the return and erasure of personal data under this Data Processing Agreement.

## 14. Breach and liability

If the Processor does not fulfil its obligations under this Data Processing Agreement or under the GDPR or other applicable privacy legislation, it is considered a breach of this Data Processing Agreement and the Main Agreement. In case of such breach, the Controller may terminate the Main Agreement with immediate effect. The Processor will still be obliged to return and erase personal data processed on behalf of the Controller pursuant to the provisions in section 13 above.

The Controller can claim compensation for financial loss, including administrative fines and claims for compensation directed at the Controller, suffered as a consequence of the Processor’s breach of its obligations under this Data Processing 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 sub-processor, the Processor shall remain fully liable to the Controller.

## 15. Duration of the agreement

This Data Processing Agreement applies for as long as the Main Agreement is in force, or until the Processor’s obligation to provide services to under the Main Agreement is terminated for other reasons.

## 16. Contacts

The contact persons for the Processor and the Controller for questions and communications related to this Data Processing Agreement are set out in Appendix 1.

## 17. Choice of law, disputes, and legal venue

The parties’ rights and obligations under this Data Processing Agreement are determined in full by Norwegian law. Any disputes arising out of this Data Processing 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 the Processor is another 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 Data Processing Agreement is made in 2 – two copies, one for each party.

|  |  |
| --- | --- |
| Place and date: | Place and date: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  On behalf of the Controller | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  On behalf of the Processor |
| Name: | Name: |
| Position: | Position: |

## Appendix 1

## Purposes of the processing

[Describe the purpose of the processing. This will be provision of the services under the Main Agreement. Give a summary of which services the Main Agreement cover.]

## Processing activities

[Describe the types of processing activities, for example collection, analysing, testing, archiving, etc.]

## 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.]

1. **Instructions**

[Formulate an instruction for the dataprocessing that states how data is to be collected, sent, shared, analysed, stored, which digital tools are to be used, etc.]

1. **Information security**

[Provide a specification of security measures implemented, stating appropriate technical, physical and organizational safety measures to achieve a level of security appropriate in relation to the risk, to prevent unauthorized or unlawful access, alteration, erasure, damage, loss or unavailability.]

## Sub-processors within the EU/EEA

|  |  |
| --- | --- |
| **Name** | **Processing activity** |
| [Schibsted] | [Marketing] |
|  |  |
|  |  |

## Sub-processors outside the EU/EEA

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

## Contacts

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

Contact person for the Processor: [Name, e-mail, phone]