**Personal data processing agreement**

SU XX-xxxx-22

On the signing date, this agreement (“the Agreement”) has been entered into between

1. Stockholm University, Corporate ID number: 202100-3062 and
2. [Counter-party] registration number: xxxxxx-xxxx

**1. Scope and background**

Processing of personal data on behalf of Stockholm University must be regulated in a Personal data processing agreement. This Personal data processing agreement has been established to ensure that the processing of personal data that is to be carried out by the Processor meets the requirements regarding personal data processing as presented by Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council.

A contract has been entered into between the Controller and the Processor for the provision of services, that may include processing of personal data.

The Processor shall process personal data solely to the extent required, to fulfil the commitments according to the Contract and in accordance with the provisions in this agreement and Applicable Law.

The Processor is aware of that situations may occur where the Controller acts as a processor. In these cases, the Processor may act as a sub-processor. The terms of this Agreement shall also apply if and when the Processer acts as a sub-processor.

**2. Definitions**

The following terms shall be understood as stated below in this Agreement.

“The Swedish Act” refers to The Act containing supplementary provisions to the EU General Data Protection Regulation (2018:218).

“Personal data” refers to the personal data that are processed by the Processor

on behalf of the Controller when providing the services of the

Contract.

“The Controller” refers to Stockholm University

“The Processor” refers to NN

“Applicable Law” refers to the Swedish Act and any other applicable and binding regulations including binding regulations from supervisory authorities

“The Contract” refers to XX

Other terms that are included in Applicable law shall have the meaning as stated, unless another meaning is clearly stated or otherwise inferred by the circumstances.

**3. Processing of Personal data**

The Processor shall process Personal data in accordance with the Contract with appendices and in accordance with this Agreement.

The Processor is obliged to keep informed of and apply Applicable Law. The Processor shall inform the Controller immediately if any given instruction is in violation of Applicable Law or any other of the EU’s Member States’ data protection provisions.

The Processor and those that process Personal data on behalf of the Processer must process the Personal data solely in compliance with this Agreement and with given instructions from the Controller and agreed routines. The Processor shall promptly inform the Controller if and when the instructions are not sufficient, and await such instructions before any further processing. Any and all instructions must be in writing to be valid.

**4. Sub-processors**

A subcontractor who processes The Controllers Personal data on behalf of the Processor is regarded as a sub-processor. The Processor may not engage a sub-processor without the written approval of The Controller, unless otherwise agreed in the Contract.

If and when the Processor engages a sub-processor the Processor is fully responsible towards The Controller for all actions and processing of the Personal data.

The Processor shall arrange and enter into a corresponding personal data processing agreement (Sub-processors agreement). A copy of the Sub-processors agreement shall be provided to the Controller upon request.

The Processor shall keep a register of the sub-processors, their contact information and location. The Processor shall supply The Controller with the information upon request.

5. **Limitations regarding transferal of Personal data**

The Processor must not without the Controller’s written instructions transfer any personal data to countries outside the EEA or to such an international organization, unless this processing is required according to European law or according to a Member State’s national law to which the Processor is subject.

If so, The Processor shall inform the Controller of the legal requirement before the data is processed unless such information is prohibited in reference to a vital interest according to Applicable law.

If and when Personal data is transferred, kept or processed in any other way outside the EEA, any such actions must be in complacence with Applicable Law, e.g. regarding protective measures.

**6. Security and information**

The Processor shall give all reasonable aid to the Controller through appropriate technical and organizational measures so that the Controller may fulfil its obligation regarding the rights of data subjects in accordance with Applicable Law. The measures shall achieve a security level that is appropriate in relation to the risk, and which is in compliance with Applicable Law.

When establishing appropriate measures and levels, special consideration shall be taken to risks arising from the Personal data being processed by the Processor, especially the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

The Processor shall, if and when a type of processing, particularly with the use of new technologies and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of data subjects, prior to the processing assist the Controller in an assessment of the impact of the planned processing. A single assessment may comprise a series of similar processing operations that entail the similar high risks.

The Processor shall upon request assist the Controller in communication with supervisory authorities, if and when the risk assessment shows that the processing is likely to include a high risk for the data subjects.

The Processor shall promptly inform the Controller of any knowledge regarding that personal data has been processed in violation of instructions from the Controller, the Agreement or Applicable Law.

The Processor shall promptly inform the Controller of any personal data breaches.

The processor shall aid the Controller to ensure that the responsibilities are fulfilled regarding (i) security, (ii) Incident reports of personal data breaches, (iii) information to the data subjects regarding personal data breaches, (iv) assessment of likely consequences of the personal data breach.

The Processer accepts the high standards regarding security for Personal data, considering the Controllers operations and status as a governmental authority.

The Processor shall, when the Contract is concluded and this Agreement is no longer valid, as instructed, delete or return all data that contains personal data on all media, and delete all existing copies, unless continued storage at the Processor’s is required according to European law or Member States’ national law. Deletion shall take place in such a way that personal data cannot be recreated.

The Processor shall ensure that all employees, consultants, any sub- processors and others that the Processor is responsible for, that process the personal data under the Agreement, are informed of the forms for the processing, the security procedures and the confidentiality that may apply for the personal data in question.

The Processor shall ensure that authorization control is correct.

**7. Audit**

The Controller has the right to, itself or through an auditor, conduct an audit or other measures of that the Processor’s processing of personal data complies with this Agreement.

In such an audit or measure, the Processor shall provide the Controller with the needed assistance.

**8. Disclosure of information**

If and when a data subject or a supervisory authority requests information from the Controller or the Processor, regarding the processing of personal data, the parties shall cooperate and exchange information to the necessary extent.

If a data subject or a supervisory authority requests information from the Processor regarding the processing of Personal data, the Processor shall refer the request to the Controller.

The Processor must not disclose any Personal data without written consent from the Controller, except if there is an order to do so from a relevant authority or if the Processor is compelled thereto according to mandatory legislation.

The Processor shall promptly inform the Controller of any contacts with a supervisory authority that regards, or may affect, the processing of Personal data. The Processor may not act on behalf of the Controller towards any data subject or supervisory authority.

**9. Confidentiality**

The Processor must not disclose any Personal data, information regarding the processing of Personal data, or other information due to this Agreement or the position of Processor, except if there is an order to do so from a relevant authority or if the Processor is compelled thereto according to mandatory legislation. The Processor must promptly inform the Controller of any forthcoming disclosure of such information in writing and request that the data should be confidential. This obligation shall remain even after the Agreement is no longer valid.

The Processor is also obliged to ensure that any persons authorized to process the personal data are bound by a corresponding statutory obligation of confidentiality and/or have entered into a sufficient agreement of confidentiality.

**10. Liability**

The Processor shall compensate for all damage that is caused the Controller through the Processor’s processing of personal data outside of or in conflict with this Agreement, with the Contract or with the Controller’s written instructions. The same applies if the damage has arisen as a result of the Processor not having fulfilled its obligations under Applicable Law.

This liability is limited to damage caused the Controller and/or a Third Party due to intent or negligence. The liability is also limited to direct damages.

In addition, the liability is limited to a maximum of 150 per cent of the total invoicing (all services of the Contract) in the calendar year that the damage arose. This limitation of liability for damages does not apply if the damage was caused due to intent or gross negligence.

**11. Amendments**

In order to be valid, amendments and modifications shall be prepared in writing and be signed by authorized persons for both parties.

The Controller has however the right to, after informing the Processor, change the instructions for the processing.

**12. Validity and termination**

This Agreement applies from its signing until all processing of Personal data on the behalf of the Controller has ended in accordance with the Contract, or until the Agreement has been otherwise terminated. A mutual period of notice of three months shall apply.

Upon termination of the Contract and/or this Agreement, The Processor shall, as instructed, delete or return all data that contains personal data on all media, and delete all existing copies, unless continued storage at the Processor’s is required according to European law or Member States’ national law. Deletion shall take place in such a way that personal data cannot be recreated.

If the Contract is replaced with a corresponding contract without entering into a corresponding new Personal data processing agreement, this Agreement shall also be valid for the new contract.

**13. Disputes and Applicable law**

Disputes regarding the interpretation or application of the Agreement shall be in accordance with what is stated in the Contract.

Two identical copies of this agreement have been prepared, of which each Party has taken one.

**Place and date Place and date**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_