**Data Processing Agreement**

This Data Processing Agreement for scientific research purposes (hereinafter the **“DPA”**) is made as relating to [define here the purpose of this DPA] (hereinafter the **“Purpose”**), and is entered into by and between:

**Aalto University Foundation sr**, [add name of the school and department]

whose registered office is located at P.O. Box 11000, 00076 AALTO, Finland

Business ID number 2228357-4

(hereinafter the **“Controller”**)

Contact person: [add name, phone and email];

and

**[add official name of the organization]**

whose registered office is located at [add address]

Business ID number [add Business ID number]

(hereinafter the **“Processor”**)

Contact person: [add name, phone and email];

hereinafter jointly referred to as the **“Parties”** and individually as a **“Party”**.

# **DEFINITIONS**

**“Data Protection Laws”** shall mean all applicable EU and national laws on personal data and professional privacy including but not limited to General Data Protection Regulation 679/2016 (hereinafter the “GDPR”), in force from time to time.

**“Model Contract Clauses”** shall mean the Standard Contractual Clauses (Data Controller–Data Controller or Data Controller–Data Processors) in force from time to time released by the European Commission. The current Standard Contractual Clauses (Data Controller–Data Processors) are located at <http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc>.

Other terms in capitals used in this DPA have the same meaning than defined in the GDPR.

# **GENERAL**

This DPA is made for scientific research purposes only and shall be agreed and signed between the Controller and Processor before any Personal Data is transferred to or processed by the Processor.

In this DPA the Controller and Processor agree on and specify the terms and conditions on Processing of Personal Data according to which Processor Processes Personal Data for and on behalf of the Controller in connection of the Purpose. The Parties undertake to comply with the Data Protection Laws in all their actions and operations.

# **ROLES AND OBLIGATIONS OF THE PARTIES**

The Controller agrees to comply with the obligations set out in the Data Protection Laws. Accordingly, the Parties understand and agree that the Controller shall use only such Processors in the Processing of Personal Data, that provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the Data Protection Laws, and ensure the protection of the rights of the Data Subjects.

The Processor shall only process Personal Data on behalf of the Controller and only in accordance with the documented instructions given by the Controller, including with regard to transfers of Personal Data to third country or an international organisation, unless required to do so by the law to which the Processor is subject to; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

If the Controller had given to the Processor a permission to use a sub-processor in the Processing, then the Processor’s sub-processor, that under this DPA participated in the Processing, would also act as a Processor on behalf of the Controller, and the obligations and liabilities applicable to a Processor, as set out in this DPA and the Data Protection Laws, would be applied to such Processor’s sub-processor.

The Controller will provide to the Processor information on the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects. The Parties agree that aforementioned information will be provided by the Controller in the **Appendix 1.**

The Controller will provide the Processor with written instructions concerning the Processing of Personal Data. The Processor expressly agrees to comply with such instructions of the Controller immediately after receipt of such instructions. The Controller may amend, update and revise such instructions at any time. The instructions may also include information, guidelines, instructions and obligations related to data security and technical and organizational measures.

# **OBLIGATIONS OF THE PROCESSOR**

## **INSTRUCTIONS FROM CONTROLLER**

The Processor expressly understands and agrees that the Processor is not authorized to Process Personal Data for its own purposes or purposes that are not in accordance with the written instructions given by the Controller. In the event that the Processor believes that the Controller’s instructions conflict with the requirements of the Data Protection Laws or other EU or Member State laws, **the** Processor **must immediately inform the** Controller giving full details of the problem and cease all Processing of the affected Personal Data (other than securely storing those Personal Data) until revised instructions are received thereof in writing.

## **CONFIDENTIALITY**

The Processor shall take all reasonable steps to ensure the reliability and integrity of any Processor’s personnel who have access to the Personal Data and ensure that the Processor’s personnel i) are aware of and comply with the Processor's duties under this subsection 4.2, ii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party, unless directed in writing to do so by the Controller, or as otherwise permitted by this DPA.

The Processor shall ensure that all persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

In the event of a request by a supervisory or other authority to receive Personal Data, the Processor shall, if legally permitted, notify the Controller without undue delay prior to any disclosure of Personal Data to such authority.

## **TECHNICAL AND ORGANIZATIONAL MEASURES**

The Processor shall implement appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access. The Processor shall ensure a level of security appropriate to the risk in order to secure the data processing taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and shall comply with the Controller’s written instructions and any updates of such instructions.

The Processor shall document all the agreed and implemented technical and organizational measures and takes care of that the documentation is up to date.

Details of appropriate technical and organizational measures taken by the Controller are stated in the **Appendix 2.** Parties shall evaluate the measures and their sufficiency on regular basis.

## **DATA SUBJECT’S RIGHTS**

The Processor shall notify in writing the Controller of all requests of Data Subjects concerning the exercising of the Data Subject's rights under the Data Protection Laws.

The Processor understands and agrees that requests concerning exercising of such rights may require the Processor at its own cost to assist the Controller with notifications and communications to the Data Subject, execution of the access rights of the Data Subject, rectification or erasure of the Personal Data, execution of restrictions of Processing and/or the right to data portability, as set out in the Data Protection Laws.

## **ASSISTING THE DATA CONTROLLER**

The Processor shall assist at its own cost the Controller, upon the request of the Controller, with complaints lodged by the Data Subjects with the data protection authority, the performance of the data protection impact assessment and possible prior consultation, as set out in the Data Protection Laws. In addition, upon the request of the Controller, the Processor shall assist the Controller in the process of obtaining of the data protection certification for a reasonable compensation.

## **NOTIFICATIONS**

The Processor shall notify the Controller in writing without undue delay and at the latest within seventy-two (72) hours after it receives from a Data Subject (or third party on his/her behalf) a Data Subject’s any request, complaint or communication relating to the Controller's obligations under this DPA or any communication from any regulatory authority in connection with Personal Data or a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by the Data Protection Laws.

The Processor shall provide the Controller with full cooperation and assistance within the timescales reasonably required by the Controller in relation to any such complaint, communication or request made.

The Processor shall notify the Controller in writing immediately after becoming aware of an actual, threatened or potential data security breach and at the latest within 24 hours upon the technical discovery of such breach of Personal Data. The Processor shall, if a breach of security occurs, immediately take all reasonable steps necessary to remedy such breach or protect the Personal Data against any breach or threat and prevent an equivalent breach in the future. Furthermore, the Processor shall notify the Controller within the same time period of any substantial fault, error or problem situations in their services, which may result in a risk to the rights and freedoms of natural persons.

The Processor shall provide in such notification at least the following information:

(a) describe in clear and plain language the nature of the Personal Data breach including, the categories and number of Data Subjects affected and the categories and approximate number of Personal Data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the Personal Data breach;

(d) describe the measures taken and proposed to be taken by the Controller to address the Personal Data breach, including, measures to remedy or mitigate such breach.

## **KEEPING RECORDS AND DEMONSTRATING COMPLIANCE WITH THE DATA PROTECTION LAWS**

The Processor **(and its data protection officer) shall keep records of its Processing of Personal Data**, including, without limitation, all Personal Data breaches, comprising the facts and effects of such breach and any remedial action taken.

The Processor shall make available to the Controller all information necessary to demonstrate its compliance with the obligations laid down in this DPA and the Data Protection Laws and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated or authorized by the Controller.

# **SUB-PROCESSORS**

If the Processor operates through or uses sub-processor(s) in the Processing of Personal Data, such sub-processing shall be governed, in addition to the Agreement, also by the terms and conditions of this DPA.

The Processor shall cause its its sub-processor(s), which take part in the Processing of Personal Data on behalf of the Controller, to comply with the obligations of the Data Processor under this DPA and the Data Protection Laws.

The Processor shall not engage a sub-processor for Processing of the Personal Data without a prior written consent of the Controller.

[By this DPA, the Controller authorizes **[add sub-processor(s) to be used]** as Processor’s sub-processor(s).]

# **CROSS-BORDER DATA TRANSFERS**

The Parties expressly agree that the Personal Data shall not be transferred outside the European Economic Area (hereinafter “EEA”) or any country not deemed adequate by the European Commission pursuant to Article 25(6) of Directive 95/46/EC (hereinafter jointly “**Restricted Countries**”), without a prior written consent given by the Controller. The current list laid down by European Commission of third countries ensuring an adequate level of protection are located at:

<http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>

In case the Controller consents to such transfer of the Personal Data to Restricted Countries, Personal Data can be transferred to third countries only with appropriate transfer agreement in compliance with EU Commission’s current Model Contract Clauses in force and/or other current requirements regarding transfer of Personal Data in force at the time of the transfer.

If the Data Protection Laws change and the Model Contract Clauses do not provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals, then the Controller shall have the right to decide, what legal instrument will be applied by the Parties to provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals in the transfer of Personal Data. If there is not such applicable legal instrument, then the Controller shall have the right to immediately interrupt, prevent and cancel the transfer of Personal Data to Restricted Countries.

Accordingly, if the Processor is located in the Restricted Countries, then the Processor shall sign the Model Contract Clauses as the data importer. If the Processor located in the EEA wants to transfer the Personal Data to the Restricted Countries, and if the Controller agrees to give the consent for such action, then the Processor shall ensure that the data importer located in the Restricted Countries signs the Model Contract Clauses with the Controller i.e. the data exporter.

# **OTHER RIGHTS AND OBLIGATIONS**

The Processor shall not acquire any rights in the Personal Data and will keep the Personal Data separate from other data held or stored by or under the control of the Processor.

[The Processor shall hold and shall cause its sub-processors to hold throughout the term of this DPA a satisfactory level of and insurance cover with a reputable insurer to cover the Processor’s obligations to the Controller.]

The Processor shall indemnify the Controller and keep the Controller indemnified in full against all direct losses, damages, injury, costs and expenses (including legal and other professional fees and expenses) awarded against or incurred or paid by the Controller as a result of or in connection with any claim made against the Controller in respect of any liability, loss, damage, injury, cost or expense sustained by the Controller's employees or agents or by any customer or third party to the extent that such liability, loss, damage, injury, cost or expense was caused by, relates to or arises from the Processing of Personal Data as a consequence of a breach or negligent performance or failure or delay in performance of this DPA by the Processor, its personnel or sub-processors.

If the Processor’s sub-processor breaches, violates or neglects this DPA and/or the Data Protection Laws, the Processor shall remain fully responsible and liable to the Controller for the performance of the obligations of the DPA and the Data Protection Laws.

If the Data Protection Laws require amendments to this DPA, the Parties agree to comply with such changes in the Data Protection Laws and negotiate and make such amendments to this DPA.

Neither Party shall do any act that puts the other Party in breach of its obligations set out in this DPA and, subject to subsection 4.1, each of the Parties shall have the right and obligation to comply with the Data Protection Laws. Any actions of complying with the Data Protection Laws, that are in conflict with this DPA, shall not be considered as a breach of obligations under this DPA.

The Parties expressly understand and agree that in order to comply with the Data Protection Laws, the Controller shall have the right to suspend, or discontinue any Processing of Personal Data, if the Controller determines at its sole discretion that such Processing of Personal Data would not be or is likely not to be in accordance with the Data Protection Laws.

Any amendments and modifications to this DPA shall be made in writing and shall be effective only when signed by the authorized representatives of the Parties.

# **TERM AND TERMINATION**

This DPA shall enter into force from the signature thereof (electronic version to be sufficient) but it shall have retroactive effect from the date when the Processor started Processing Personal Data on behalf of the Controller, if applicable. The term of this DPA shall be the duration of the Personal Data Processing specified in the **Appendix 1.**

Each Party shall be entitled to terminate the DPA with immediate effect if the other Party is in material breach of the terms of this DPA. For the clarity, any breach, violation or negligence of this DPA by the Processor shall constitute a material or substantial breach of this DPA, in consequence of which the Controller has the right to resort the remedies provided in this DPA.

Upon the expiration or termination of this DPA, the Processor shall, in accordance with and at the Controller’s sole discretion, delete or return all Personal Data to the Controller and delete existing copies, unless the applicable, mandatory laws require the storage of the Personal Data. The Controller may provide more detailed instructions to the Processor in this regard, such as a request to provide evidence in implementing previously mentioned obligations.

# **APPLICABLE LAW AND DISPUTE RESOLUTION**

This DPA shall be construed and governed by the laws of Finland, excluding its choice of law provisions. Any disputes under this DPA that cannot be resolved through negotiation, shall be submitted to District Court of Helsinki for resolution, unless otherwise agreed.

# **APPENDICES**

Controller determines the purposes of Processing Personal Data.

**Appendix 1** The details of the Personal Data, including but not limited to, subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects.

**Appendix 2** The technical and organizational measures that Controller applies to the Personal Data Processing.

# **SIGNATURES**

**Aalto University Foundation sr**

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**[add name of the Organization]**

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[MODEL OF APPENDIX 1]

**APPENDIX 1 - DETAILS OF PERSONAL DATA PROCESSING**

1. **SUBJECT-MATTER OF PROCESSING**

[please describe the type of Personal Data and categories of Data Subjects]

1. **NATURE AND PURPOSE OF PROCESSING**

[please describe the nature and purpose]

1. **DURATION OF PROCESSING**

[please specify the duration]

[MODEL OF APPENDIX 2]

**APPENDIX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES**

The Processor shall take all security measures required pursuant to Article 32 of the GDPR, in particular with the following measures:

[please specify the technical and organizational measures **e.g pseudonymisation and encryption of the Personal Data,** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, **redundancy and back-up facilities**, **applicability of possible code of conduct or approved certification mechanism]**