DATA PROTECTION APPENDIX (CONTROLLER TO CONTROLLER)

This Data Protection Appendix (this "Appendix") is executed between [….] on the behalf of itself [and any or all its affiliates] ("Publisher"), the [….], [the two latter individually "University", and collectively "Universities"], and all [three] together the "Parties".

This Appendix is a stand-alone agreement between the Parties and is applied to the extent that the [University as a Controller TAI Universities as joint Controllers] of Personal Data Process Personal Data that Publisher discloses to the [University TAI Universities] for the scientific research purposes defined in the Licensing Agreement dated on [xx.yy.20..] ("Agreement"). In the event of any conflict or inconsistency between this Appendix and the existing Agreement between the Parties, this Appendix shall prevail.

The Parties agree that with regard to the Processing of Personal Data under this Appendix, Publisher is an independent Data Controller, and and the [University is a Controller TAI Universities are joint Controllers]. [The Universities shall arrange their practices and responsibilities as joint Controllers of the Personal Data that Publisher discloses to them in a separate agreement.]

For the sake of clarity, the [Universities'] right to Process or otherwise use Personal Data that Publisher discloses to the [Universities] to be Processed as [joint Controllers TAI Controller] is limited only to the Processing for the scientific research purposes contemplated and defined by the Agreement.

Capitalised terms shall have the meanings set out in Annex 2 hereto.

1. PROCESSING OF PERSONAL DATA

1.1. Publisher's obligations

Publisher is responsible for compliance with its obligations as stipulated in the Laws.

1.2. The [Universities'] obligations

The [Universities] shall without additional charge payable by Publisher comply with

(i) the Laws; and
(ii) written instructions of Publisher or Supervisory Authority. In cases where the [Universities] consider that Publisher's instructions are in conflict with the Laws, they shall immediately in writing notify Publisher.

The [Universities] shall use or Process Personal Data only for the scientific research purposes contemplated and defined by the Agreement and shall not use or Process Personal Data or data derived from it for any other purpose (except to the extent required by applicable legislation).

The [Universities] shall not during or after the term of the Agreement, disclose or transfer, or enable access to or Processing of, Personal Data to or by any Third Party.

Except as specified in the Agreement and this Appendix, the [Universities] shall not have any rights to Personal Data.

1.3. Use of subcontractors by the Universities

Publisher has approved the list of the [Universities'] subcontractors. The list is in Annex 1. The [Universities] may engage subcontractors that Process Personal Data only with Publisher's prior written approval and provided that

(i) such engagement will be under a written contract; and

(ii) the contract will require the subcontractor to comply at the minimum level with the same obligations applicable to the [Universities] under this Appendix.

The [Universities] shall always remain fully liable for the acts and omissions of its subcontractors.

1.4. Data retention

As a Controller the [Universities] are liable under the Laws for

(i) not retaining or otherwise Processing Personal Data for longer than it is necessary for the scientific research purposes contemplated and defined by the Agreement; and
(ii) defining time limits for the period for which Personal Data will be retained.

Upon termination or expiry of the Agreement, the [Universities] shall

(i) destroy any Personal Data from all computer hardware (including storage media), software, and databases used by the [Universities] to Process the Personal Data; and
(ii) confirm in writing that this has been done.

1.5. Data disclosures

Unless such notification is prohibited by applicable law, each Party shall immediately notify the other Parties of any requests from governmental authorities regarding access to the Party's Personal Data, and if possible, the Parties shall collaborate in good faith in designing a response to such a request.

2. INTERNATIONAL TRANSFER OF PERSONAL DATA

The [Universities] shall not transfer or Process Personal Data in a non-EEA country unless

(i) Publisher has provided a prior written consent to such transfer. Transfers disclosed in Annex 1 are considered to have been approved by Publisher; and

(ii) the Laws and other legal requirements regarding the Processing of Personal Data outside the EU/EEA countries are complied with.

If required by the Laws, the [Universities] shall (and shall procure that any subcontractors shall) enter into the appropriate Model Clauses. The [Universities] shall promptly terminate the transfer of Personal Data or to pursue a suitable alternate mechanism that can lawfully support the transfer, in case the statutory mechanism under this Appendix is modified, revoked, or held in a court of competent jurisdiction to be invalid.

3. DATA SECURITY AND SAFEGUARDS

The [Universities] shall

(i) implement and maintain appropriate organizational, operational, managerial, physical and technical measures to protect the Personal Data and any other Publisher's data against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access, especially where the Processing involves the transmission of data over a network;

(ii) assess the measures necessary to ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(iii) ensure that technical measures comply with industry standards and best practices such as ISO 27001/27002 (or equivalent);

(iv) limit access to the Personal Data to authorized and properly trained personnel with a well-defined "need-to-know" basis, and who are bound by appropriate confidentiality obligations; and

(v) ensure by technical and organizational means that Personal Data is not Processed for different purposes.

4. SELF-ASSESSMENTS AND AUDITS

On an annual basis Publisher may request a review of the [Universities]' security documentation and/or a written self-assessment report on the [Universities]' compliance with this Appendix.

In addition Publisher (or an independent Third Party appointed by Publisher) may conduct an audit on the Processing by the [Universities] according to audit plan upon forty-five (45) days' prior written notice. Publisher may also request the [Universities] to audit the [Universities]' subcontractors respectively. If such audit reveals that the Processing is not in compliance with this Appendix, the [Universities] shall, at their sole expense take all necessary corrective measures. Publisher may verify the compliance by another audit at any time after the implementation of such corrective measures.

Publisher shall bear the costs for the audits. However, if the audit reveals a violation or breach of this Appendix by a University, the University shall without delay remedy the breach and reimburse Publisher for the costs arising from the audit.

5. HANDLING OF PERSONAL DATA BREACHES

In the event of a Personal Data Breach or any other threatening enforcement proceeding against the University pertaining to the Processing of Personal Data, the University shall

(i) provide Publisher with an accurate written notice at (….) promptly and in without undue delay upon becoming aware of the Personal Data Breach;

(ii) work for quickly resolving the issue, and preventing further losses;

(iii) provide any notices to a Supervisory Authority and Data subjects as mandated by the Laws; and

(iv) upon Publisher's prior request, provide any appropriate remedial services to the Data subjects.

Breach by the University (or its subcontractors, as the case may be) of its obligations under this Appendix will be deemed as a material breach.

6. RIGHTS OF THE DATA SUBJECTS

As [Data Controller TAI joint Data Controllers] the [Universities] are liable under the Laws for ensuring rights of the Data subjects.

7. INDEMNIFICATION

The [Universities] hereby agree to indemnify, defend and hold Publisher harmless from and against all damage, loss, liability, expense (including, without limitation, reasonable expenses of investigation and fees of consultants, auditors and attorneys) or any lack of funds, assets or rights arising out of or resulting from the [Universities]' failure to protect Personal Data against a Personal Data Breach or to comply with any of its obligations under this Appendix.

In the event of any Third Party Claim, the University in question shall give a written notice to Publisher. Such written notice shall be given within thirty (30) days from the date from which the University became aware of the Third Party Claim. In respect of any such Third Party Claim the University shall:

(i) not make any admission of liability, agreement, settlement or compromise in relation thereto without prior informing and consulting with Publisher of the Third Party Claim;
(ii) will avoid, defend or appeal such Third Party Claim to the extent it is evidently necessary to protect Publisher's interests regarding Personal Data; or
(iii) alternatively permit Publisher to take or conduct any such action itself in the manner Publisher deems appropriate, in which event the University shall ensure that Publisher is given all authorizations and all assistance necessary (including access to relevant information) to enable Publisher to defend any Third Party Claim and to properly conduct any litigation resulting therefrom. Publisher shall reimburse the University for any reasonable out-of-pocket expenses incurred by the University in connection therewith.

8. TERM AND TERMINATION

This Appendix shall come into effect on the last date of acceptance/signature of the Agreement by the [Universities].

As a stand-alone agreement, this Appendix shall remain in full force as long as Personal Data is Processed by the [Universities] as [joint Data Controllers TAI Data Controller] for the scientific research purposes defined in the Agreement. Obligations which by their nature should survive the termination or expiration of the Appendix, shall so survive.

9. GOVERNING LAW

This Appendix is governed by the laws of Finland. Any disputes arising from or in connection with this Appendix shall be brought exclusively before the Helsinki district court.

Annex 1: Instructions for Processing Personal Data

This Annex includes Publisher's instructions provided to the [Universities] for the purposes of Processing Personal Data. The instructions will be provided and/or up-dated during the term of Agreement.

1. Data Controller	Publisher is a Controller. As defined above and as applicable, the [Universities are joint Controllers TAI University is a Controller].
2. Data subjects: The Personal Data transferred concern the following categories of data subjects (please specify):	
3. Categories of data: The Personal Data Processed concern the following categories of data (please specify):	
4. Special categories of data: The Personal Data Processed concern the following special categories of data (please specify):	
5. Approved subcontractors: The Personal Data will be Processed by the following parties (please specify):	
6. Countries/locations data will be processed: The Personal Data will be Processed (remotely accessed or hosted) in following countries/locations (please specify):	Finland
7. Other instructions: Other instructions regarding Processing: (Please add reference to, or list, instructions received from Publisher, for example regarding agreed practices on storage, transfer, deletion, encryption or pseudonymization of data) Further instructions on Processing may also be communicated by email.	

Annex 2: Definitions

"**Controller**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Data subject**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Third Party**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Laws**"	applicable laws relating to data protection, privacy and security, including without limitation EU Directive 95/46/EC EU and Directive 2002/58/EC (collectively the "EU Directives") and any amendments, replacements or renewals thereof, including but not limited to EU General Data Protection Regulation 2016/679, as well as all binding national laws implementing the EU Directives and other applicable binding data protection, privacy or data security directives, laws, regulations and rulings when Processing Personal Data for the scientific research purposes defined in the Agreement
"**Model Clauses**"	the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the transfer of Personal Data to Processors established in third countries under the EU Directives and any amendment, replacement or renewal thereof by the European Commission.
"**Personal Data**"	any information as defined in Article 4 of the EU General Data Protection Regulation (2016/679), relating to a Data subject which is sent to at least one University, is accessed by a University or is otherwise Processed by a University on Publisher's behalf or as a Controller for the scientific research purposes defined in the Agreement
"**Personal Data Breach**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Processing**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Processor**"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"Supervisory Authority"	As defined in Article 4 of the EU General Data Protection Regulation (2016/679)
"**Technical and organizational security measures"**	measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing
"**Third Party Claim"**	any claim, action or proceeding by a Third Party, Data subject or Supervisory Authority against at least one of the Universities concerning the infringement of Laws relating to Publisher employees (current and former), job applicants, external workforce or customers (prospective, current and former)