**DATA PROCESSING AGREEMENT**

[Name of procurement and other possible identifying information] (hereinafter the ”Procurement”)

This Data Processing Agreement (hereinafter the “Agreement”) shall constitute an integral part of the Procurement Contract [record identifier] referred to above (hereinafter the “Procurement Contract”).

1. **Parties**

This Agreement is entered into by and between the following Parties:

1. Tampere University Foundation sr operating as Tampere University (business ID 2844561-8; hereinafter the “Data Controller”)

1. [Party]

Business ID

address (hereinafter the “Data Processor” or “Processor”)

The Parties shall hereinafter be individually referred to as a “Party” and collectively referred to as the “Parties”).

1. **Scope of this Agreement**

This Agreement shall apply to the processing of all personal data that is carried out by the Data Processor on behalf of the Data Controller in connection with the Procurement or as part thereof. The provisions of this Agreement shall take precedence in the event of any inconsistencies between the Procurement Contract and this Agreement.

1. **Definitions**

The term *Data Protection Laws* shall mean all laws that apply to the processing of personal data, including but not limited to the Finnish Personal Data Act (523/1999), the European Union’s General Data Protection Regulation (EU 2016/679, hereinafter the “GDPR”) and possible amendments thereof, and any and all decisions, instructions, and information notices concerning the processing of personal data that are issued by data protection authorities or courts of law.

Unless otherwise provided in this Agreement, the terms *personal data*, *personal data processing*, *data processor*, *data controller*, *data subject*, *third party*, *data register*, *data protection authority* and *data protection breach* shall have the meaning set forth in the GDPR.

1. **Scope of processing personal data**

For the purpose of carrying out activities pursuant to the Procurement Contract, the Data Controller hereby authorises the Data Processor to process personal data on behalf of the Data Controller in accordance with the provisions set out in the section titled Description of processing activities in this Agreement.

1. **Duration of processing**

The Data Processor shall be authorised to process personal data under this Agreement for as long as the Data Processor provides the Data Controller with the services specified in the Procurement Contract.

1. **General obligations of the Data Controller**

The Data Controller shall act as the data controller referred to in the Data Protection Laws.

The Data Controller determines the purposes for which and the manner in which personal data are processed. The Data Controller shall be accountable for complying with the obligations that are imposed on data controllers under the Data Protection Laws.

The Data Processor acknowledges and understands that the Data Controller may only use the services of data processors who take appropriate technical and organisational security measures to ensure that all personal data are processed in compliance with the Data Protection Laws and that the rights of data subjects are protected.

1. **General obligations of the Data Processor**

The Data Processor shall act as the data processor as referred to in the Data Protection Laws.

The Data Processor shall comply with the procedures and regulations set out in the Data Protection Laws regarding the processing and protection of personal data. The Data Processor shall ensure that the services provided under this Agreement comply with the Data Protection Laws, the provisions set out in the Procurement Contract and, in particular, the regulations concerning data protection by design and default.

The Data Processor shall implement appropriate technical and organisational measures to ensure that personal data are processed on behalf of the Data Controller in accordance with the Procurement Contract and the practices agreed between the Parties. The purpose of the technical and organisational measures is to guarantee that personal data are lawfully processed and to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The Data Processor shall not process or otherwise exploit personal data received under the Procurement Contract for purposes other than that which is strictly necessary for the performance of its obligations under the Procurement Contract.

The Data Processor shall designate a data processing officer or a contact person who will serve as a point of contact that handles all requests and inquiries from the Data Controller. The Data Processor shall provide the contact details of the data processing officer of contact person to the Data Controller in writing.

The Data Processor shall process personal data on behalf of the Data Controller. The Data Processor warrants that it has the necessary expertise and resources to process personal data in compliance with the Data Protection Laws and protect the rights of data subjects. The Data Processor hereby guarantees that all the appropriate technical and organisational measures relating to the processing of personal data are taken in compliance with the Data Protection Laws and the provisions set forth herein.

1. **Use of subprocessors**

The Data Processor may not subcontract the performance of any of the services hereunder to another data processor (hereinafter “Subprocessor”) without the Data Controller’s explicit prior written consent. The Data Processor shall inform the Data Controller of any and all intended changes concerning the addition or replacement of Subprocessors, thereby giving the Data Controller the opportunity to object to such changes. A Subprocessor may not process personal data on behalf of the Data Controller until the Data Controller has approved said Subprocessor.

The Data Processor shall ensure that its Subprocessor complies with the data protection obligations referred to herein and signs a written data processing agreement. The Data Processor shall remain fully liable and responsible for any action, omission or negligence of its Subprocessor.

The Data Processor shall, at the Data Controller’s request, promptly provide the Data Controller with a list of all its Subprocessors and the locations where personal data are processed.

1. **Guidelines for processing personal data**

The Data Processor hereby agrees to only process personal data in accordance with documented instructions provided by the Data Controller and only to the extent specified therein. The Data Processor shall ensure that all persons who are acting under the authority of the Data Processor and have access to the personal data referred to in this Agreement only process personal data in strict compliance with the instructions provided by the Data Controller.

When the Procurement Contract comes into force, the Procurement Contract and its appendices (including this Agreement) shall constitute the Data Controller’s instructions referred to herein. During the term of the Procurement Contract, the Data Controller may provide the Data Processor with amended, updated or revised instructions concerning the processing of personal data.The Data Processor hereby agrees to comply with any amended, updated or revised instructions provided by the Data Controller. If compliance with amended, updated or revised instructions necessitates measures that significantly exceed the level specified in the Data Protection Laws and the Data Processor incurs more than minor additional expenses for taking the necessary measures, the Data Processor shall be entitled to receive reasonable compensation, as agreed in advance between the Parties, for the additional work.

The Data Processor shall ensure that all persons who are acting under the authority of the Data Processor and have access to the personal data referred to in this Agreement are aware of their obligations pertaining to the processing of personal data and only process personal data in accordance with the Procurement Contract, the terms and conditions set out in this Agreement and the instructions provided by the Data Controller.

The Data Processor shall notify the Data Controller forthwith if the instructions provided by the Data Controller, in the Data Processor’s opinion, are incomplete or violate the Data Protection Laws. Upon receipt of such notice, the Data Controller shall review the instructions and promptly provide the Data Processor with revised instructions or a written confirmation that the original instructions comply with the Data Protection Laws.

1. **Obligation to assist and data subjects’ right of access**

The Data Processor shall, upon the Data Controller’s request, provide the Data Controller with all the information that the Data Controller needs to demonstrate compliance with the data protection regulations and fulfilment of the Data Controller’s obligations. The Data Processor shall, among other things, document all processing activities performed under this Agreement and the Procurement Contract in an electronic format and, upon the Data Controller’s request, promptly provide the Data Controller with information about processing activities. The Data Processor shall be obligated to assist the Data Controller with preparing and maintaining descriptions and documents, such as data protection impact assessments, and conducting prior consultations as set out in the GDPR.

The Data Processor shall take appropriate technical and organisational measures to assist the Data Controller in the fulfilment of the Data Controller’s obligations under the Data Protection Laws pertaining to data subject rights. The Data Processor agrees to promptly notify the Data Controller of any subject access requests made by data subjects. The Data Processor shall not respond to subject access requests. The Data Processor shall assist the Data Controller in fulfilling its obligation to respond to subject access requests. To help the Data Controller respond to subject access requests, the Data Processor may have to, for example, assist the Data Controller in communicating with data subjects, enforcing data subject rights, rectifying or deleting personal data, restricting the processing of personal data, or transferring a data subject’s personal data to a different IT environment.

Any expenses incurred by the Data Processor in meeting the obligations referred to herein shall be included in the service fee specified in the Procurement Contract. If, however, compliance with the obligation to assist the Data Controller necessitates measures that significantly exceed the level specified in the Data Protection Laws and the Data Processor incurs more than minor additional expenses in the course of taking these measures, the Data Processor shall be entitled to receive reasonable compensation, as agreed in advance between the Parties, for the additional work.

1. **Information security**

The Data Processor hereby agrees to comply with the information security requirements set out in the Procurement Contract and the Data Protection Laws and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the Data Processor’s processing activities. While assessing the appropriate level of security, the Data Processor must consider the risks presented by processing and, in particular, the protection of personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

The Data Processor shall without undue delay notify the Data Controller of any suspicions that a personal data breach has taken place or is currently taking place. The Data Processor’s notification of a personal data breach must include sufficient and comprehensive information about the breach, including a description of the personal data breach, the impact of the personal data breach, the measures that have or will be taken in response to the personal data breach and other details requested by the Data Controller. The Data Processor shall also report to the Data Controller all processing activities that violate the Data Protection Laws, the Procurement Contract, this Agreement or the instructions provided by the Data Controller.

1. **Data Controller’s right to conduct data protection audits**

The Data Controller, or an auditor authorised by the Data Controller, shall be entitled to perform audits and inspections that are necessary to confirm the compliance of the Data Processor and possible Subprocessors with their obligations under the Data Protection Laws. The Data Processor shall ensure that its Subprocessors sign agreements that ensure that the Data Controller is also authorised to audit the Data Processor’s Subprocessors. An audit may include, among other things, requests for information, inspections and other applicable audit activities. The Data Processor shall ensure that data protection audits can also cover its Subprocessors that process personal data on behalf of the Data Controller to deliver the services specified in the Procurement Contract.

Audits may be conducted once a year unless the Data Controller has a valid reason for conducting audits more frequently. The Data Processor undertakes to assist the Data Controller with audits and participate in them. The Data Controller shall be responsible for its own and the auditor’s expenses incurred in the course of data protection audits. The Data Processor shall be responsible for its own expenses incurred in the course of data protection audits.

Audits shall, if possible, be conducted during the Data Processor’s normal opening times and with as little inconvenience to the Data Processor as possible. In case any problems or weaknesses are detected during an audit, the Data Processor shall be responsible for resolving the problems or weaknesses at its own expense.

Alternatively, the Data Processor may, with the Data Controller’s prior consent, demonstrate its regulatory compliance by presenting an up-to-date audit report or certificate issued by an external, independent and impartial auditor.

1. **Transfer of personal data**

The Data Processor may not transfer personal data outside the EEA, or make personal data held in the EEA accessible in countries outside the EEA, without the Data Controller’s prior written consent. The Data Processor shall ensure that a possible transfer of personal data outside the EEA, or the provision of access to personal data in countries outside the EEA, is conducted in compliance with the Data Protection Laws.

1. **Confidentiality**

The Data Processor undertakes to treat in strict confidence all personal data, and all information related to the processing thereof, to which the Data Processor gains access pursuant to this Agreement or the Procurement Contract. The confidentiality obligations shall survive the termination or expiration of the Procurement Contract.

The Data Processor warrants and undertakes that all persons who are working under the authority of the Data Processor and are authorised to process the personal data referred to in this Agreement agree to strictly comply with the confidentiality obligations referred to herein or are under an appropriate statutory obligation of confidentiality.

1. **Liability**

The Data Processor shall be solely and fully liable for any losses, damages or costs incurred by the Data Controller, a data subject or a third party due the Data Processor’s breach of the obligations set forth in this Agreement or in the Data Protection Laws.

The Data Processor shall be liable for any and all damages and costs resulting from corruption, destruction or loss of personal data or other materials held by the Data Controller, including costs associated with restoring or recreating such data.

Possible limitations of liability set out in the Procurement Contract or any other documents shall not apply to the Data Processor’s liability under this Agreement.

Where a Party has paid full compensation for damage suffered by a data subject as a result of a violation of the Data Protection Laws, that Party shall be entitled to claim back from the other Party that part of the compensation corresponding to the other Party’s part of responsibility for the damage. The amount of compensation that a data subject can receive for a personal data breach is determined based on Article 82, Paragraph 2 of the GDPR or similar provisions set out in other Data Protection Laws.

1. **Validity and termination of this Agreement**

This Agreement shall become effective after both Parties have signed the Procurement Contract, and this Agreement shall apply as of the date when the Data Processor starts processing personal data referred to in this Agreement on behalf of the Data Controller This Agreement shall expire when the Procurement Contract expires or is terminated. Notwithstanding the foregoing, this Agreement shall remain in full force and effect for as long as the Data Processor processes personal data on behalf of the Data Controller.

After the Procurement Contract expires or is terminated, the Data Processor shall, at its own expense, promptly return to the Data Controller or destroy all personal data that the Data Processor has received on behalf of the Data Controller. The obligation to destroy personal data shall apply to all documents, data, information, disks, external storage media and any and all storage media that contain data included in the scope of this Agreement, unless the Court of Justice of the European Union or the legislation of a Member State requires the retention of personal data. This obligation also applies to possible reproductions, copies and backup copies.

1. **Other terms and conditions**

This Agreement may only be amended by mutual written agreement signed by both Parties. The updating of the instructions for processing personal data referred to in Section 9 above shall not be considered as an amendment to this Agreement.

Description of processing activities

**This description of processing activities constitutes an integral part of the Data Processing Agreement. This description specifies the assignment to process personal data on behalf of the Data Controller as set out in the Procurement Contract and the Data Processing Agreement.**

|  |
| --- |
| **Categories of data subjects whose personal data will be processed**  Staff (including visiting researchers and lecturers)  Students  Job candidates  Student applicants  Research participants  Contact persons of stakeholder groups (partners, service providers, customers, public authorities)  Other, please specify: |
| **Categories of personal data that will be processed**  **Basic information**, including:  Name  Personal identity number  Age/date of birth  Gender  User ID  Signature  IP address  Other, please specify:  **Contact information**, including:  Home address or location  Work/company address  Email address/fax number  Phone number  Job title/role  Other, please specify:  **Employment information**, including:  Employee number  Position and information about tasks, qualifications, internships, educational background, length of service, working hours, absences and annual leave  Salary, bank account, taxation  Professional development reviews and other assessments  Campus access control records  Information about recruitment, such as job applications, CVs, interviews and the results of aptitude tests  Other, please specify:  **Students’ information**, including:  Student number  Information about the right to study, including the institution, degree programme, major and minor subjects and the duration of the right to study  Attendance records  Information about studies, including course registration, completed courses, course completion dates, course content, academic record, grades and assessments, completed degrees  Information about student admission, including registration for an entrance examination, participation in an entrance examination, exam answers, marks and grades, and the results of aptitude tests  Other, please specify:  **Information about stakeholder**s, including:  Information about interactions with customers, partners and service providers  Information about the location where services or products are delivered or where research is conducted  Payments and invoices  Other, please specify:  **Information about research participants**, including (please note that identifying information and all research data, such as survey results, interviews, recordings, videos etc. including pseudonymised data are considered personal data):  **Other personal data** (please specify): |
| **Special category data that will be processed (if applicable)**  Special category data will not be processed.  The following special category data, as defined in Articles 9 and 10 of the GDPR, will be processed under this Agreement:  Racial or ethnic origin  Political opinions  Religious or political beliefs  Trade union membership  Genetic data  Biometric data used for identification purposes  Health data  Data concerning a person’s sex life or sexual orientation  Criminal convictions and offences |
| **Nature of and the purpose(s) of processing on behalf of the Data Controller**  [You can refer to the Procurement Contact or otherwise describe the activities or the purpose of the Contract, such as:  - jointly delivered services  - research project or plan  - process  - collaboration between the parties  In addition, describe the IT systems, services or tools that will be used in the course of the processing activities and where personal data will be processed.  Try to describe the processing activities as clearly and concretely as possible.] |
| **Procedure and deadline for deleting personal data after the contract expires**  [Describe how long the categories of personal data will be retained and when they will be deleted.  Specify the agreed deadlines and the practices/procedures for **returning** or **destroying** personal data.  Upon the Data Controller’s request, the Data Processor and Subprocessor must provide the Data Controller with a signed document where they confirm that all personal data has been returned or destroyed in accordance with the contract. |
| **Describe the goals, nature and duration of processing activities carried out by a Subprocessor or Subprocessors.** |
| **Location of personal data (if the location is outside of the EU/EEA, please also fill out the section “Transfer of personal data”)**  ☐ EU/EEA member states  ☐ USA  ☐ Other, please specify: |
| **Transfer of personal data**  The processing of personal data outside of the EU/EEA is not permitted.  Personal data may be processed outside of the EU/EEA under the following:  The European Commission’s decision on an adequate level of protection for personal data in a country located outside of the EU  Standard Contractual Clauses  Binding Corporate Rules  Clear and explicit consent of the data subject  Other, please specify: |
| **Other terms and conditions** |
| **Signatures**     |  |  |  | | --- | --- | --- | | Place and time | | | |  | | | |  |  | | Place and time | | | |  | | | |  |  | |