Resource Allocation Platform Service Contract

Contract Number: S732/21-96300-01

Date:

between

VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center, registry code 61989100, address 17. listopadu 2172/15, 70800 Ostrava, Czech Republic, represented by Assoc. Prof. Vít Vondrák, Managing Director of IT4Innovations (hereinafter the **Customer**),

and

the University of Tartu, registry code 74001073, address Ülikooli 18, 50090 Tartu, represented by Professor Jaak Vilo, Head of the Institute of Computer Science,

have entered into the following contract:

1. Used terms in this Contract

1.1. Allocating body - The entity that decides on the allocation of the resources to Projects

1.2. API - *application programming interface*, a communication interface, which can be used for data exchange between systems

1.3. ISKE - three-level reference security system for information systems. ISKE is based on the IT Baseline Protection Manual (IT-Grundschutz) published by the German BSI (German Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security). ISKE describes three levels of security - low (L), medium (M) and high (H). The corresponding security level is determined for the data by assigning security classes (security sub-classes). The security classes are determined based on the confidentiality of the information, the integrity of the information, the availability of time-critical information, and the permissible severity of the consequences of information delays. (iske.ria.ee)

1.4. Fixing time - Time from receiving a message about an incident until the recovery of the service or the operation of IT systems or devices or applications.

1.5. Office hours - From Monday to Friday 9:00 to 17:00, except for national holidays.

1.6. Project - A Project is an object with one or more allocations on one or more resources. The Project has a number of consumable units assigned for each of the allocations. It is assigned to a PI, has one or more optional proxy-PI and one or more members. The Project is time-limited by the lifespan.

1.7. Puhuri Core - resource allocation platform, the central database that keeps track of the components of the Puhuri Services, with information on for example resources, Projects, Puhuri accounts, usage, etc

1.8. Response time - Time from receiving a message about an incident until the UT HPCC commences their action.

1.9. Resource - A Resource object represents a compute cluster, storage system, or cloud resource.

1.10. Service - in this context it means Puhuri Core

1.11. Service interference - Situation in which the service as described in the Contract or the operation of IT systems or devices or applications is restricted (is interfered).

1.12. Service interruption - Situation in which the service as described in the Contract or the operation of IT systems or devices or applications cannot be continued (is interrupted).

1.13. User - A user is an entity (a real person or a machine) that uses the Resource. A User can belong to zero, or more Projects.

1.14. UT HPCC - University of Tartu High Performance Computing Centre

2. The object of the Contract

2.1. The object of this Contract is the provision of Service by the UT HPCC to the Customer. For the purpose of this Contract, resource allocation service means the provision of the platform, network connections, and other additional services that are necessary for accessing and using Puhuri Core by Customer. Customer can make API requests towards Puhuri Core to check if a user is registered and if the user has rights to login to the Puhuri Core. The Allocating body can decide which users can manage their projects.

2.2. With this contract, the Allocating body gets access to the Puhuri Core service. This will allow them to manage Resources in the scope allocated to them upon the LUMI Project agreements.

2.3. Users, who have access to allocated resources, their personal data is stored. The source of the personal data is the MyAccessID service provided by GEANT. Personal data processing is described in the appendix "AGREEMENT ON THE PROCESSING OF PERSONAL DATA".

3. Procedure for the provision of the Service

3.1. The Service is deemed to have started on 01.01.2022

4. Terms of service provision

4.1.   Description of the service level agreement (SLA):

Criticality level	Description of situation	Maximum time of response	Maximum fixing time	Maximum allowed interruption of the service in a month
None	Service provided as planned	Up to 8 hours within office hours	-	-
Low	Service not directly interfered	Up to 4 hours within office hours	Up to 8 hours within office hours	Up to 16 hours within office hours
Medium	Service partly interfered	Up to 2 hours within office hours	Up to 16 hours round the clock	Up to 16 hours round the clock
High	**Interrupted service**	Up to 2 hours round the clock	Up to 8 hours round the clock	Up to 8 hours round the clock

4.2.   If the performance of pertinent obligations is not possible or practical (e.g., the initial diagnosis proved wrong), the parties agree through their contact persons on the future action and the time of fixing the specific failure.

4.3.   The service is not deemed to be interrupted or interfered and the response and recovery times do not apply in cases when the incidence is caused by the Customer's action or failure to act, by scheduled works or force majeure.

4.4.   The parties shall refrain from any action that interferes (or may interfere) or limits (or may limit) or causes (or may cause) damage to the security of the other party's system, infrastructure or communication network. The parties shall also ensure that the current software of their infrastructure is up to date and secure.

4.5.   In the case of any communication disruption or technical problem caused by the action or omission of the Customer, the Customer removes technical problems themselves or shall reimburse the UT HPCC any costs incurred by the UT HPCC for the work performed to restore data transmission.

5. Maintenance works

5.1.   The UT HPCC shall inform the Customer and all Service users of all scheduled works one (1) week in advance through the portal environment and/or by an email.

5.2.   The UT HPCC shall perform any planned maintenance works with minimal interference in the service.

5.3.   During planned maintenance works, the operation of the service may be interfered, but any interference caused by planned maintenance is not considered as non-compliance with the service (it is regular maintenance).

5.4.   Downtimes caused due to upgrades for fixing critical security issues are not considered SLA violations. In the case of critical security upgrades, UT HPCC reserves the right to apply the upgrades with minimal notice.

6. Rights and obligations of the UT HPCC

6.1.   The UT HPCC shall ensure uninterrupted 24-hour availability of services.

6.2.   The UT HPCC shall ensure that the service platform and components are updated.

6.3.   All obstacles in the service area of the UT HPCC that prevent the Customer from using the Service and are beyond the control of the Customer shall be removed by the UT HPCC within two (2) hours at the UT HPCC's expense, counting from the time the UT HPCC becomes aware of the obstacle.

6.4.   The UT HPCC provides access to a resource allocation platform for allocating bodies, which have rights to manage allocation shares.

6.5.   The UT HPCC provides API connectivity for allocation bodies to connect their portal or system with the Puhuri Core service.

6.6.   In the provision of the Service, the UT HPCC shall comply with the requirements of the security level M (medium) and shall ensure confidentiality as required for security subclass S2 in the security system ISKE.

7. Notification of incidents, faults and requests

7.1.   The Customer shall immediately notify the UT HPCC of any problems with the use of the Service.

7.2.   If the Service does not function, the Customer shall contact the UT HPCC control centre by a notification to the following address: support@hpc.ut.ee.

7.3.   The Customer shall forward all requests and observations to the UT HPCC using the following address: support@hpc.ut.ee.

8. Liability of the Parties

8.1. If the UT HPCC fails to comply with the deadline specified in clause 4.1, the Customer will be credited to the extent of the fee for one (1) month on the basis of a corresponding request of the Customer.

9. Service fee

9.1. UT HPCC provides the Service for free until May 31, 2022.

9.2. From June 1, 2022 Service fee will be dependent on the available Service plans.

10. Changes to Contract

10.1. The terms and conditions of this contract may be changed at any time by mutual agreement of the parties. Such modification shall be effective upon the signing by both parties of an amendment to this contract encompassing those changes.

10.2. If Customer decides to use the Service after the date specified in clause 12.2, Customer must notify UT HPCC at least one (1) month before the date specified in clause 12.2 about the request of Service continuation. UT HPCC will provide available Service plan options to Customer after Service continuation request.

11. Termination of the Contract

11.1. Either party may terminate this contract at any time without any reason, upon presentation of a one hundred and eighty (180) days' notice given to the other party.

11.2. This Agreement shall terminate on May 31, 2022.

12. Contact persons

12.1. Both parties appoint a contact person as their representative, who has the right to represent the contracting party in contractual matters.
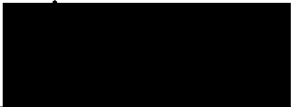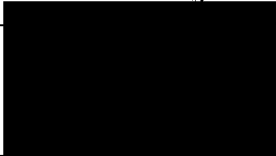
12.2.

12.3.

13. Appendices

13.1. APPENDIX 1 - AGREEMENT ON THE PROCESSING OF PERSONAL DATA

13.2. APPENDIX 2 - DESCRIPTION OF PERSONAL DATA PROCESSING MEASURES

Parties signatures

	Controller	Processor
Organization:	VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center	University of Tartu Institute of Computer Sciences
Typed or Printed Name:	Assoc. Prof. Vít Vondrák	Prof. Jaak Vilo
Title:	Managing Director	Head of the Institute
Signature:	███████	███████

APPENDIX 1 - AGREEMENT ON THE PROCESSING OF PERSONAL DATA

to "Resource Allocation Service Contract" no S732/21-96300-01

between

VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center
(hereinafter the **Controller**)

and

University of Tartu
(hereinafter the **Processor**)

1. General

1.1. When processing personal data, the Controller shall serve as the controller in GDPR context and the Processor shall serve as the processor in GDPR context of personal data, unless otherwise specified with regard to the purpose of processing personal data. In these terms and conditions, personal data refers to any personal data processed under this Agreement and for which the Controller serves as the controller in GDPR context of such personal data.

1.2. This Appendix specifies the terms and conditions for processing personal data and data protection that are binding for the Controller and Processor, according to which the Processor, at the behest of the Controller, processes personal data on behalf of the Controller in addition to the terms and conditions of the Agreement.

1.3. The Parties shall be obligated to comply with applicable personal data processing and data protection legislation in their operations. Furthermore, the Parties' processing of personal data must comply with the required EU General Data Protection Regulation (GDPR) (EU) 2016/679 b.

1.4. The Processor shall provide the Controller with the contact details of contact person or person in charge of data protection in writing.

2. Roles of the Parties in processing personal data

2.1. The Controller shall serve as the controller stipulated in legislation on personal data processing and data protection when specifying the purpose and measures of personal data processing. The Parties understand that, as a

controller, the Controller shall only use personal data processors who take adequate protective measures in the implementation of appropriate technical and organizational arrangements in order to ensure that any and all processing meets the requirements laid out in applicable legislation on personal data processing requirements laid out in the GDPR. Furthermore, both Parties shall ensure the protection of the rights of data subjects.

2.2. Any sub-processors, Processor may use, are obliged to process personal data solely to the extent relevant to the Processor's activities under the Agreement.

2.3. The object, nature and purpose of personal data processing, the types of personal data and data subject groups and the obligations and rights of the Controller and Processor are described in "APPENDIX 2 - DESCRIPTION OF PERSONAL DATA PROCESSING PURPOSES" appendix as well as documentation or other Controller guidelines, which are binding upon the Processor and drafted during the contractual provision of service. The Processor is obligated to comply with the terms, conditions and descriptions of personal data processing specified in the Agreement, Description of personal data processing purposes, documentation and guidelines. The Controller shall be responsible for ensuring the maintenance and availability of guidelines.

2.4. If no Description of personal data processing measures (as specified in Section 2.3) has been drafted or it is incomplete, the Controller shall draft or complete the Description of personal data processing measures; if necessary, the Controller will do so in cooperation with the Processor.

2.5. The Processor shall notify the Controller if its specified guidelines are incomplete or if the Processor believes said guidelines are in violation of applicable law.

2.6. The Processor shall take the appropriate measures for protecting personal data processed under this Agreement in accordance with GDPR, stated Agreement requirements and the Controller's written guidelines in order to ensure the confidentiality, integrity and availability of personal data.

2.7. At the behest of the Controller, the Processor shall provide the necessary data for drafting and maintaining a report on the processing measures being carried out by the Controller as well as data required by the Controller to meet its other disclosure obligations. The Processor shall provide the data mentioned above at no extra charge.

3. Subcontractors that process personal data

3.1. If the Agreement does not stipulate the use of subcontractors for processing personal data, the Processor shall refrain from using the services of a subcontractor in the processing of personal data without the express written consent of the Controller. The Processor shall notify the Controller in writing of all planned changes that will affect the addition or changing of subcontractors serving as personal data processors. The Processor shall also give the Controller an opportunity to object to such additions or changes.

3.2. Insofar as the Processor uses subcontractors to process personal data in its operations, the terms and conditions specified in this appendix and the Agreement itself shall be applied to any subcontracting employed.

3.3. The Processor and its subcontractors, which serve as the processors of the Controller's personal data on behalf of the Controller, shall comply with all obligations applicable to the processors of personal data described in this appendix. The Processor is obligated to make agreements with its subcontractors in order to ensure their compliance with the terms and conditions stated in this appendix.

3.4. If the subcontractors used by the Processor process personal data and, in doing so, violate or fail to honor the provisions specified in the Agreement, this appendix or applicable legislation, the Processor shall be held accountable for such breaches of contract or acts of negligence as if they were committed by the Processor itself. If the data processing subcontractor fails to meet its data protection obligations, the Processor shall still be held fully liable to the Controller. If the Controller justifiably deems that a subcontractor used by the Processor fails to meet its data protection obligations, the Controller reserves the right to demand that the Processor changes subcontractors.

4. General obligations of the Processor

4.1. The Processor shall process personal data in accordance with the Agreement and the guidelines specified by the Controller.

4.2. The Processor shall ensure that all persons working in its employ who are authorized to process personal data have agreed to comply with the confidentiality obligation or a statutory confidentiality obligation applicable to them.

4.3. Furthermore, in accordance with the requirements concerning personal data protection, data security and confidentiality stipulated in the Agreement, the

Processor shall be obligated to take the appropriate technical and organizational measures in order to ensure a security level commensurate with the risk involved when processing personal data, taking into consideration: new technology and implementation costs; the nature, scope, context and purposes of the processing involved; and risks varying in probability and severity that affect the rights and freedoms of natural persons. Furthermore, the Processor shall comply with the guidelines set by the Controller and any updates made to these guidelines by the Controller.
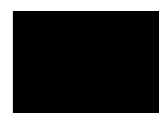
4.4. The Processor shall take measures in order to ensure that each natural person working under the Processor that has access to personal data only processes data in accordance with the Agreement and the Controller guidelines.

4.5. The Processor documents the measures agreed upon and carried out, and ensures that the documentation is kept up to date. The Parties assess the technical and organizational measures to be taken and their adequacy on a regular basis.

4.6. The Processor shall be required to notify the Controller, without undue delay, of all data subject requests concerning the exercising of data subject rights in accordance with valid legislation and the GDPR.

4.7. The Processor shall be obligated to assist the Controller with the appropriate technical and organizational measures so that the Controller will be able to fulfill its obligation to respond to requests concerning the exercising of data subject rights. The Processor understands that requests concerning the exercising of these rights may require the Processor's assistance in:

    4.7.1. informing and communicating with data subjects;

    4.7.2. ensuring that data subjects are given access rights;

    4.7.3. revising or deleting personal data;

    4.7.4. setting restrictions on processing;

    4.7.5. and/or transferring personal data from one system to another.

4.8. The Processor obligations specified in this section are included in the price of the service being provided under a customer-specific agreement and no extra charges shall be paid for the measures specified above.

4.9. The Processor shall ensure that any personal data it processes is in such a commonly used and machine-readable form that said data can be automatically extracted from one system and transferred to another system in cases where this is technically possible.

4.10. If necessary, the Processor shall be required to assist the Controller in:

    4.10.1. conducting a GDPR Data Protection Impact Assessment (DPIA);

4.10.2. prior consultations (if any);

4.10.3. and acquiring data protection certification (if any).

4.11. The Processor shall be entitled to additional charge for additional work not listed in the Contract at person-work hour rates specified in the Appendix 3 and in accordance with the agreed work order procedure.

4.12. The Processor shall be obligated to delete or return all of the Controller's personal data to the Controller when the provision of services involving personal data processing has ended. The Processor shall delete any existing reproductions, except in cases where European Union law or member state legislation requires that personal data be maintained. The Controller may provide more detailed guidelines to the Processor with respect to this.

4.13. The Processor shall only process personal data within the agreed service provision area. Stipulations in the Agreement and these terms and conditions concerning the processing of personal data shall also apply to facilitating access to personal data, for example, via an administrative and supervisory connection. Personal data may be transferred to countries outside the European Economic Area under an appropriate agreement in accordance with European standard clauses valid at a given time and/or other requirements concerning the transfer of personal data valid at that time. Unless otherwise agreed concerning the service provision area, the Processor reserves the right to process the Controller's personal data only within the European Economic Area.

4.14. The Processor shall provide the Controller with access to all data that is necessary for showing compliance with the obligations specified in this appendix. Furthermore, the Processor shall permit the Controller or an auditor authorized by it to conduct audits and participate in them. More detailed terms and conditions concerning audits are provided in the Agreement as well as the appended security agreement signed between the Parties.

5. Special Processor obligations

5.1. Unless otherwise agreed, the Processor shall be required to maintain a record of revisions, deletions or processing restrictions involving the personal data of data subjects. This record shall be handed over to the Controller or third parties authorized by the Controller upon request.

6. Data breaches

6.1. Unless otherwise agreed, the Processor (including any of its sub-processors) shall immediately notify the Controller in writing of any personal data breaches it becomes aware of, using the procedure specified by the Controller. The Processor is obliged to notify Controller without undue delay (and in any event no more than 12 hours after discovery) of any cases of accidental or unauthorized access and any other material disruptions or problems in the service provided by the Processor that might have an impact on the status and rights of data subjects.

6.2. The Processor shall provide the Controller with at least the following information on the data breach:

6.2.1. a description of the personal data breach, including, if possible, the data subject groups involved and estimated numbers as well as the personal data type groups and estimated numbers;

6.2.2. the data protection officer or another supervisory person, who can provide additional information;

6.2.3. a description of the probable consequences of the personal data breach; and

6.2.4. a description of the measures proposed or taken by the Processor in response to the personal data breach and, if necessary, the measures to be taken to mitigate any adverse impacts.

6.3. The Processor shall take appropriate measures to address the data breach, including measures to mitigate its possible adverse effects and work with the Controller to identify a root cause and remediate the data incident. The Processor shall document all relevant facts relating to the breach including its effects and any remedial action is taken, and keep a record thereof.
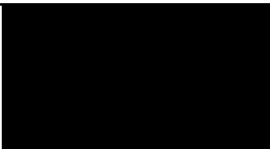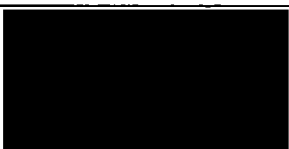
7. Other terms and conditions

7.1. The Controller reserves the right to change, add and update guidelines concerning the processing and data protection of the personal data it provides to the Processor. Said changes, additions and updates of the guidelines may consist of changes, additions or updates to technical or organizational measures concerning the processing and data protection of personal data. The Processor shall make the necessary changes in accordance with the Controller's guidelines. If the Controller's guidelines result in changes to be made by the Processor, additional costs shall be agreed upon separately and

compensated at the person-work hour rates specified in the Appendix 3. The Processor and other processors of personal data shall be obligated to comply with these changed, added or updated guidelines.

7.2. Unless otherwise specified in the Agreement service level requirements, the Processor shall be obligated to respond without undue delay of any contact made by the Controller and answer any service requests or complaints made by the Controller concerning data protection within one (1) week. However, the Processor shall respond to any data breaches without undue delay.

7.3. The liability of the Processor is specified in the Agreement as well as in applicable legislation. The Processor is liable to the Controller or any other person, including data subjects and data protection authorities, including the Data Protection Inspectorate of Estonia.

7.4. The Parties hereby understand that data protection legislation is in transition at the time of the Agreement and this appendix. If the legislation in question or recommendations, guidelines or provisions concerning said legislation or its interpretation are amended in a way that affects the status or obligations of the Controller or the obligations or responsibilities specified in this appendix, the terms and conditions contained in this appendix may be, if necessary, revised with respect to said amendments. If this appendix is changed in a way that results in additional costs for the Processor, compensation of said costs shall be agreed upon separately in accordance with the person-work hour rate specified in the Appendix 3. The Processor and other processors of personal data shall be obligated to comply with the inspected appendix in question.

Parties signatures

	Controller	Processor
Organization:	VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center	University of Tartu Institute of Computer Sciences
Typed or Printed Name:	Assoc. Prof. Vít Vondrák	Prof. Jaak Vilo
Title:	Managing Director	Head of the Institute
Signature:		

APPENDIX 2 - DESCRIPTION OF PERSONAL DATA PROCESSING PURPOSES

to "Resource Allocation Service Contract" no S732/21-96300-01

between

VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center
(hereinafter the **Controller**)

and

University of Tartu
(hereinafter the **Processor**)

1. Purpose

This document describes all processing measures taken by the Processor as a personal data processor on behalf of the Controller, the types of personal data and the personal data to be processed. This document (the "Appendix 2") is attached to and forms part of the Agreement between VSB-Technical University of Ostrava, IT4Innovations National Supercomputing Center and University of Tartu.

2. Types of personal data and data subject groups

The Parties hereby agree that the Processor shall, on behalf of the Controller, process the following personal data contained in the Controller person register in order to provide the service specified in the Agreement:

- User identity and contact information:
    - Provided by Identity Provider (IdP): given name and surname, common user identification number, institutional email address, ssh key and organizational affiliation.
    - Provided by user: mobile phone number
- Technical information: equipment information pertaining to the services provided, including technical identifications, user name, user roles, user ssh key, user IP address, web browser type and version, operating system, contact information, communications data and metadata, and technical transactions related to the services provided, including system and application log data.
- Security information: security log data, system surveillance data and security incident data.

3. Nature and purpose of processing

The Parties hereby agree that the Processor will process the subject's personal data only for:

- Handling resource allocations and user project management for accessing LUMI supercomputer, and other resources defined by the Resource Allocator
- Managing accounting information for the granted resources
- solving technical issues with the allocation portal;
- investigating and solving data breach occurrences;
- resolving and replying to user service and support requests;
- data protection impact assessment.

4. Duration of personal data processing

The Processor shall process the personal data specified in this Appendix during the duration of Data Access Agreement no S732/21-96300-01.