Annex No. 6

to the Special Part of the Contract for the Public Procurement-Sale of services

**ARRANGEMENT ON PROCESSING OF PERSONAL DATA**

**GENERAL PART**

**1. CONCEPTS AND DEFINITIONS**

* 1. **Personal Data** means the personal data specified in the Special Part, which the Data Controller authorises the Data Processor to process for the purpose and within the time limit set out in the Special Part.
  2. **Data Processor** means a natural person or legal entity providing the services referred to in the Special Part.
  3. **Data Controller** means a State Enterprise Centre of Registers acting as a data controller or a data processor representing the data controller referred to in the Special Part.
  4. **JIRA** means a software tool for managing project, product and software development, maintenance tasks and resources.
  5. **Confidentiality Commitment** means a commitment in the form prescribed by the Data Controller to protect the secrecy of the data processed by the State Enterprise Centre of Registers and to comply with the data security requirements, which shall be signed by the authorised persons of the Data Processor prior to commencement of the processing of personal data.
  6. **Regulation (EU) 2016/679** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
  7. **Service Agreement** means an agreement for the provision of services signed between the Service Provider and the Service Recipient as specified in the Special Part, on the basis of which the Arrangement is concluded as an integral part thereof.
  8. **Service Recipient** means the State Enterprise Centre of Registers.
  9. **Service Provider** means a natural person or legal entity providing the services referred to in the Special Part.
  10. **Arrangement** means an integral part of the Service Agreement, consisting of a General and Special Parts, which, in accordance with Article 28 of Regulation (EU) No 2016/679, establishes the rights and obligations of the Data Controller and the Data Processor with regard to the processing of personal data on behalf of the Data Controller.
  11. **General Part** means the part of the Arrangement, which lays down general terms and conditions for the processing of personal data applicable to the Parties thereto.
  12. **Special Part** means the part of the Arrangement, which lays down special terms and conditions for the processing of personal data applicable to a particular Data Processor.
  13. **Parties** means the Data Controller and the Data Processor jointly.

1. **SUBJECT-MATTER OF THE ARRANGEMENT**

2.1. The Data Controller hereby shall entrust the Data processor with the processing of personal data under the terms and conditions laid down therein.

1. **RIGHTS AND OBLIGATIONS OF THE PARTIES**
   1. Data Controller shall:
      1. Be obliged to ensure that the processing of personal data entrusted to the Data Processor has a legal ground;
      2. Have the right to provide documented instructions throughout the period of processing of personal data in addition to the instructions for the processing of personal data set out in the Arrangement. Such instructions may be provided in writing at the address of the registered office of the Data Processor referred to in point 2 of the Special Part, or by e-mail, or recorded in JIRA (where access rights have been granted to authorised persons of the Data Processor);
      3. Have the right to verify, in addition to and/or by other means than those referred to in point 3.2.9, how the Data Processor is processing personal data and/or fulfils its obligations hereunder; such verification may be carried out when the Parties agree on the scope, manner, cost and time thereof. The Data Controller shall have the right to engage an independent auditor to carry out the additional verification. In any case, if the Parties agree on such additional verification, it shall have to meet the following requirements:
         1. Verification must be related only to the processing of personal data under the Arrangement;
         2. The Data Controller must inform the Data Processor of the request to carry out an additional verification within a reasonable period of time, which must be at least 5 working days;
         3. The additional verification must be carried out in such a way that it does not interfere with the normal activities of the Data Processor;
         4. In the event that confidential information of the Data Processor may be accessed during verification, the Data Controller undertakes to protect the confidential information of the Data Processor at the request of the Data Processor.
   2. Data Processor shall:
      1. Process personal data in accordance with the Data Controller’s instructions set out hereunder and any other instructions provided in writing (including in an electronic form) by the Data Controller, except where processing of the data is required by the legislation of the European Union or a Member State of the European Union to which the Data Processor is subject (in which case the Data Processor shall inform the Data Controller of these requirements, except in cases where the legislation prohibits the provision of such information on the grounds of an overriding reason of public interest);
      2. Ensure that persons authorised to process personal data are committed to confidentiality and have signed a Confidentiality Commitment in the form provided by the Centre of Registers;
      3. Take all the measures required under Article 32 of Regulation (EU) 2016/679, i.e., ensure by technical and organisational means the security, confidentiality, integrity and accessibility of personal data processed on behalf of the Data Controller, protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access, and against any other unauthorised processing, as well as secure transmission of data over computer networks. The security measures to be implemented by the Data Processor, as set out in point 6 of the Special Part of the Arrangement ‘Instructions on the security of the processing of personal data’, as well as, depending on their appropriateness to the nature of the processing of personal data, shall be, including but not limited to:
         1. Pseudonymisation and/or encryption of personal data;
         2. Ability to ensure the continuous confidentiality, integrity, accessibility and resilience of data processing systems and services;
         3. Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
         4. Process for regular testing, inspection and evaluation of technical and organisational measures ensuring the security of processing of personal data;
      4. Ensure that it is going to engage a sub-processor to carry out specific processing activities on behalf of the Data Controller only with the permission of the Data Controller as set out in the Special Part, and that the sub-processor engaged is going to be subject to the same data protection obligations as set out in this Arrangement;
      5. Given the nature of data processing, assist the Data Controller to the extent possible by applying appropriate technical and organisational measures to fulfil the obligation of the Data Controller to respond to requests to exercise the rights of the data subject set out in Regulation (EU) 2016/679. If the Data Processor receives a request from a data subject for the exercise of the data subject’s rights set out in Articles 12-22 of Regulation (EU) 2016/679, it must forward the request to the Data Controller without delay, but at the latest within 3 working days, by the e-mail address referred to in point 7 of the Special Part;
      6. Assist the Data Controller in ensuring compliance with the obligations laid down in Articles 32-36 of Regulation (EU) 2016/679, taking into account the nature of the data processing and the information available:
         1. Not later than within 24 hours after a personal data breach has become apparent, inform the Data Controller in writing at the addresses indicated in point 7 of the Special Part of the personal data breach that has occurred and provide a notification, including the information listed in Article 33(3) of Regulation (EU) 2016/679, and take measures to immediately stop the breach and prevent further damage caused by the personal data breach as well as mitigate the consequences of the personal data breach. If it is not possible to provide all the information at the same time, the information must be provided in phases without delay. Upon request of the Data Controller, the Data Processor shall provide, within the specified period, additional information necessary for the Data Controller to assess the circumstances of the personal data breach, including, but not limited to, an extract from the Data Processor’s personal data breach log;
         2. Upon request of the Data Controller, provide, within a time limit specified by the Data Controller, the information necessary for the Data Controller to carry out a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679, including provision of information if the Data Controller decides to contact the State Data Protection Inspectorate for prior consultation;
      7. After completing the provision of services related to data processing, and taking into account the instructions of the Data Controller provided for in the Special Part, delete or return to the Data Controller all personal data and delete existing copies thereof, except in cases where legislation of the European Union or the Republic of Lithuania stipulates the Data Processor’s obligation to retain personal data. If the Data Processor is subject to a statutory obligation to retain personal data, the Data Processor shall, prior to processing of personal data on behalf of the Data Controller, indicate in the Special Part the applicable legislation under which the Data Processor is obliged to retain personal data;
      8. Undertakes not to copy, transfer, store or otherwise process personal data in the Data Processor’s IT infrastructure where, in accordance with the instructions provided by the Data Controller in the Special Part, it has been established that personal data shall be processed only in the Data Controller’s IT infrastructure;
      9. Undertakes to verify periodically, at its own initiative and expense, whether the respective technical and organisational measures are appropriate to the nature, scope, context and purposes of the data processing, as well as to the risks associated with the data processing with respect to the rights and freedoms of natural persons. The Data Processor may carry out this verification itself or engage an independent auditor. Upon a written request of the Data Controller, the Data Processor must provide the Data Controller with an inspection report or an extract thereof;
      10. If the Data Controller does not specify in the Arrangement or does not subsequently provide documented instructions for the transfer of personal data to a third country or to international organisations, the Data Processor shall not be entitled to carry out such transfer under this Arrangement unless the transfer of personal data to third countries or international organisations is required by the laws of the European Union or a Member State thereof, with which the Data Processor must comply, even though the Data Controller has not instructed the Data Processor to do so. In this case, the Data Processor shall inform the Data Controller of this legal requirement, indicating in the Special Part the legislation applicable to it, which obliges it to transfer personal data to a third country or to international organisations unless that legislation prohibits the transfer of such information;
      11. Having reasonable grounds to believe that the Data Controller’s instructions may infringe legal acts, shall have the right to suspend the execution of such instructions after having informed the Data Controller in writing at the addresses referred to in point 7 of the Special Part. Once the Data Controller has demonstrated conformity of instructions with the legislation or has amended them, the instructions shall be enforced.
2. **RESPONSIBILITY**
   1. The Data Controller shall be responsible for ensuring that the instructions it provides to the Data Processor regarding the processing of personal data comply with the requirements of Regulation (EU) 2016/679.
   2. The Data Processor shall be responsible for processing the personal data provided by the Data Controller in accordance with this Arrangement and the instructions of the Data Controller.
   3. If a sub-processor engaged fails to fulfil or inadequately fulfils the personal data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the fulfilment of the obligations of the sub-processor engaged.
   4. The terms and conditions of the Arrangement shall not exempt the Parties from any other obligations, to which they are subject under Regulation (EU) 2016/679 or other legislation.
3. **FINAL PROVISIONS**
   1. The Arrangement shall come into force on the date of its signing and shall be valid until the expiry of the Service Agreement.
   2. Any disagreements or disputes arising between the Parties in connection with the Arrangement shall be settled by means of negotiations, and if the Parties are unable to reach an agreement, they shall be settled in the court of the Republic of Lithuania according to the location of the registered office of the Data Controller pursuant to the laws or regulations in force in the Republic of Lithuania.

**ARRANGEMENT ON PROCESSING OF PERSONAL DATA**

**SPECIAL PART**

1. **Data Controller (Service Recipient):**

State Enterprise Centre of Registers, legal entity code 124110246, with registered office at Studentų St. 39, Vilnius, phone number (8 5) 268 8262, e-mail address info@registrucentras.lt, acting on behalf of the Data Controller Ministry of Health of the Republic of Lithuania, legal entity code 188603472, registered Vilniaus str. 33, Vilnius, phone number +370 5 268 5110, email ministerija@sam.lt.

1. **Data Processor (Service Provider):**

*[enter company name, code, registered address, phone number and e-mail address; if the Data Processor is a natural person, enter their name, surname, individual economic activity certificate number or business licence number, address of the place of residence, phone number and e-mail address]*

1. **Service Agreement:**

*[enter the name of the Service Agreement. If the Arrangement is signed later than the Service Agreement, also enter the date and number of the Service Agreement]*

1. **Provisions on the processing of personal data:**

|  |  |
| --- | --- |
| Purpose of the processing of personal data | I lot – Implementation and configuration of VNA and DICOM based services.  II lot – Modernisation of portals, web services, FHIR data structure and interface to medical images. |
| Nature of the processing of personal data and processing operations | Get familiar with the existing ESPBI IS solution and its features (ability to see personal data in the ESPBIS IS test environment).  To carry out a test run of the developed System.  Perform installation and testing of the developed System.  Migration of data to the new subsystem.  Perform warranty (with the possibility to see personal data in the ESPBI IS production environment). |
| Categories of personal data subjects | ESPBI users – patients or their representatives, healthcare professionals, persons participating in testing. |
| Types of personal data processed | The data of the ESPBI IS users are indicated in Chapter III of the Resolution of the Government of the Republic of Lithuania No. 1057 "On the Approval of the Regulations of the Information System for Electronic Health Services and Cooperation Infrastructure" of 7 September 2011.  Name, surname, personal identification number, position, contact details of the persons involved during testing. |
| Place of the processing of personal data | In the Data Controller’s IT infrastructure at Studentų str. 39, Vilnius. |
| Duration of the processing of personal data | The duration of the service contract. |
| Permission to use a sub-processor who will be engaged after the signing of the Arrangement | The Data Processor may engage a sub-processor only with the prior specific permission of the Data Controller. The Data Processor shall inform the Data Controller about a sub-processor to be engaged by sending an official letter to the address specified in point 7 of the Special Part, no later than 20 working days before the planned engagement, and the Data Controller shall give the Data Processor the written permission or objection within 10 working days at the contacts specified in point 2 of the Special Part (the letter shall be sent by post or e-mail). |
| Instructions of the Data Controller for erasure or return of personal data after the end of processing | Upon termination of the provision of services to the Data Processor that processed personal data in the infrastructure of the Data Controller, access to the information resources of the Data Controller shall be terminated immediately (on the same day). |
| Statements by the Data Processor, based on the European Union and/or the Republic of Lithuania legislation regarding mandatory retention of personal data (if applicable to the Data Processor) | *(To be completed by the Service Provider (Data Processor)* |
| Conditions for the transfer of data to third countries or international organisations | Will not be transferred |

1. **Information about sub-processors engaged at the time of signing the Arrangement: *(To be completed by the Service Provider (Data Processor)***

|  |  |  |  |
| --- | --- | --- | --- |
| Company name, name, surname | Company code/date of birth or individual economic activity certificate number | Registered address/address of the place of residence | Description of data processing |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Instructions on the security of personal data processing:**

|  |  |
| --- | --- |
| Data processing security measures | The Data Processor shall comply with the Arrangement on Applicable Organisational and Technical Cybersecurity Requirements, which are set out in a separate Annex No *[enter]* to the Special Part of the Service Agreement. |

1. **Contact details of the Data Controller:**

|  |  |
| --- | --- |
| Personal data breach notification | duomenusauga@registrucentras.lt |
| Requests for the exercise of the data subject’s rights under Articles 12-22 of Regulation (EU) 2016/679 | duomenusauga@registrucentras.lt |
| Notification of the authorisation to engage a sub-processor | **...**@registrucentras.lt and info@registrucentras.lt  ***Note\**** *The e-mail address of the Product Owner is entered only before the Arrangement is signed, once the Service Provider is known* |
| Other issues | **...**@registrucentras and info@registrucentras.lt  ***Note\**** *The e-mail address of the Product Owner is entered only before the Arrangement is signed, once the Service Provider is known* |