SPECIAL CONDITIONS OF THE CONTRACT FOR THE PUBLIC PROCUREMENT-SALE OF THE SERVICES

Contract title	Implementation and configuration of VNA and DICOM based services;	
1. PARTIES TO THE CONTRACT		
1.1. Buyer	1.1.1. Name	State Enterprise Centre of Registers
	1.1.2. Code of legal entity	124110246
	1.1.3. Address	Studentų St. 39, LT-08106 Vilnius
	1.1.4. VAT payer's code	LT241102419
	1.1.5. Transactional account	LT94 4010 0424 0005 0387
	1.1.6. Deposit bank account	LT14 7300 0101 3363 7868
	1.1.7. Bank, bank code	Luminor Bank AS Lithuanian Branch, bank code 40100
	1.1.8. Telephone	+370 5 268 8262
	1.1.9. E-mail	info@registrucentras.lt
	1.1.10. Party's representative	Director General
	1.1.11. Basis of representation	Articles of Association
1.2. Provider	1.2.1. Name	J4Care GmbH
	1.2.2. Code of legal entity	Commercial Register Number: FN 298641d
	1.2.3. Address	Enzersdorferstraße 7 2340 Mödling, Austria
	1.2.4. VAT payer's code	ATU 63646825
	1.2.5. Transactional account	IBAN 124300033643870000
	1.2.6. Bank, bank code	Volksbank Wien Bank code:43000
	1.2.7. Telephone	
	1.2.8. E-mail	
	1.2.9. Party's representative	
	1.2.10. Basis of representation	CEO
2. RESPONSIBLE PERSONS		
2.1. Buyer's contact persons responsible for the performance of the Contract, acceptance of the Services, acceptance of invoices through the information system SABIS		
2.2. Contact persons of the Provider responsible for the performance of the Contract	J te e	
3. SUBJECT-MATTER OF THE CONTRACT		
3.1. Subject-matter of the Contract	The Provider undertakes to provide the Services to the Buyer under the terms and conditions provided for in Part I of the Contract – Implementation and configuration of VNA and DICOM based services. (hereinafter referred to as the Services). The detailed description of the Services and other requirements for the Services provided shall be set out in Annex 2 to the Contract 'Technical	

	Specification' (hereinafter referred to as the Technical Specification) and in Annex 3 to the Contract 'Tender bid'.
3.2. Title and number of the Procurement	Purchase and installation of a complete MedVais modernisation solution, CVP IS No: 2254548.
3.3. Information on a project funded by the European Union or another project	Project co-financed by the European Union No. 09-033-P-0001, title "Development of the national information system for archiving and exchange of medical images and e-services based on this system (hereinafter referred to as the Project).
4. TIME LIMITS FOR THE PROVISION OF THE SERVICES AND PROCEDURE FOR THE TRANSFER AND ACCEPTANCE OF THE SERVICES	
4.1. Time limit for the provision of the Services when the Services are provided once, periodically or according to the Buyer's Order	4.1.1. The Provider undertakes to provide the Services (Part I of the Procurement object - Implementation and configuration of VNA and DICOM based services (hereinafter referred to as the Services), Additionally ordered development services (hereinafter referred to as the Additional Services), System support services (hereinafter referred to as the Support Services), **not later than within 7 months** from the date of entry into force of the Contract (in case not less than 7 months remain from the date of conclusion of the Contract until 30 April 2026) **or until 30 April 2026** (in case less than 7 months remain from the date of conclusion of the Contract until 30 April 2026). 4.1.2. The Provider undertakes to provide the Additional Development Services for 7 months from the date of entry into force of the Contract (in case not less than 7 months remain from the date of conclusion of the Contract until 30 April 2026) or until 30 April 2026 (in case less than 7 months remain from the date of conclusion of the Contract until 30 April 2026). Orders of the Services may be placed and must be completed within the time limit specified in the Order, but no later than by the end of the time limit/date specified above. 4.1.3. The Support Services shall be provided (if ordered) within the ordered term but not longer than 60 months. The Support Services shall be provided not earlier than the end of the warranty maintenance period and upon receipt of an order from the Contracting Authority (applicable only for Part I of the Procurement object).
4.2. Extension of the time limit for the provision of the Services/part thereof/phase/term	4.2.1. The Parties to the Contract shall be entitled to an extension of the term of the Services specified in point 4.1.1. but only if: 4.2.1.1. There are evidence-based obstacles or disturbances, which occurrence the Parties to the Contract have no influence on, and which they are not responsible for, and which are caused by and attributable to third parties, or other circumstances, which could not have been known to the Parties to the Contract in advance. The circumstances that justify the need to extend the term of delivery of the Services cannot in any way depend on the parties to the Contract. In each such case, the party to the Contract initiating the extension of the term of delivery of the Services shall notify the other party to the Contract thereof in writing without delay, but not later than within 5 working days, providing evidence of the existence of such circumstances. The specified circumstances shall be assessed by the other Party to the Contract, and following its consent, the time limit for provision of the Services may be extended only for the period of existence of the said circumstances **but not longer than:**

	4.2.1.1.1. **by 2026-04-30** or 4.2.1.1.2. **The term of implementation of the Project** if the term of implementation of the Project is going to be extended; however**, not longer than 6 months** or 4.2.1.1.3. **For a period not exceeding 6 months** if funding is provided not from the Project funds. 4.2.2. **The term of the provision of Additional Development Services specified in point 4.1.2. of the Special Conditions may be extended** if the Initial Contract Value specified in point 5.2 of the Special Conditions is not fully used. In this case, the Buyer shall notify the Provider in writing, indicating the period for which the time limit for provision of the Service is proposed to extend. Following the consent of the Provider, the time limit for provision of the Services may be extended only until the Initial Contract Value specified in point 5.2 of the Special Conditions of the Contract is fully used but **not longer than 6 months (the number of extensions is not limited).**
4.3. Order submission procedure	The procedure for placing Orders for additional Services is described in the Chapter 6.2 'Requirements for Ordering Services' of Annex 1 'Requirements for the Procurement Object' to the Technical Specification.
4.4. Regarding the minimum Order value or volume	Not applicable
4.5. Documents provided	The following documents must be provided (if the Provider fails to provide the specified documents, the Services shall be deemed not to comply with the contractual requirements):
	4.5.1. Statement on the Transfer and Acceptance of the Services — Yes
	4.5.2. Invoice — Yes
	4.5.3. Documents referred to in Annex 2 to the Contract 'Technical Specification' — Yes
	4.5.4. Documents referred to in Annex 1 'Requirements for the Procurement Object' to Annex 2 to the Contract 'Technical Specification' — Yes
	Failure by the Provider to provide the said documents shall be deemed to indicate that the Services do not comply with the requirements set out in the Contract.
5. CONTRACT PRICE AND PAYMENT PROCEDURE	
5.1. Method of calculating the price applicable to the Contract	Mixed pricing (fixed price and fixed fee)
5.2. Initial Contract Value and Contract Price	The Initial Contract Value shall be 3.980.000,00 EUR , excluding value added tax (hereinafter referred to as the VAT). VAT shall amount to 835.800,00 EUR The Contract Price shall be 4.815.800,00 EUR including VAT.

<table>
<tr><td></td><td colspan="2">The Initial Contract Value in this Contract shall be equal to the maximum amount of funds allocated to the procurement, excluding VAT, to procure the Services specified in the Procurement documents and in the Contract:
5.2.1. The price of the Service provision - Implementation and configuration of VNA and DICOM based services (1 set) shall be equal to the price of the tender bid, excluding VAT, for the total quantity and/or volume of the Services specified in the Procurement documents and the Contract (fixed price pricing);
5.2.2. Additional Development Services shall be purchased at the fee rates specified in the tender bid, excluding VAT. The Buyer shall procure Additional Development Services according to the need at the fee rates specified in the Contract or in its Annex No 3 'Tender bid', not exceeding the Contract price. Quantity of the Additional Development Services specified in the Contract or in its Annex No 3 'Tender bid' shall be maximum. The Buyer does not undertake to buy the maximum quantity of the Additional Development Services or any part thereof (fixed fee pricing).
5.2.3. The Buyer shall order the Support Services only if funding is received for the purchase of these Services. The Services will be ordered considering the amount of funding that was actually received and paid for at the rates set out in the Contract or in Annex 3 'Tender bid' thereto, not exceeding the total price of the Contract. The Buyer shall not be obliged to order the entire quantity of the Support Services proposed or part thereof (fixed fee pricing).</td></tr>
<tr><td rowspan="5">5.3. Recalculation of the Contract Price/fees by applying the <u>revision</u> rules</td><td colspan="2">The Contract Price/fees shall be recalculated:</td></tr>
<tr><td>5.3.1. Due to changes in the VAT rate</td><td>Yes</td></tr>
<tr><td>5.3.2. Due to changes in other charges that affect the price of the Services</td><td>No</td></tr>
<tr><td>5.3.3. Due to changes in the price level</td><td>Yes</td></tr>
<tr><td>5.3.4. According to the price changes in the Service groups</td><td>No</td></tr>
<tr><td>5.3.1. Revision of the Contract Price/fees due to changes in the VAT rate</td><td colspan="2">If during the performance of the Contract there is a change in legal acts governing the payment of VAT, which directly affect the price/fees of the Services provided by the Provider under the Contract, the Contract Price/fees shall be recalculated without changing the Service prices/fees, excluding VAT.

The recalculated Contract Price/fees shall be subject of the Arrangement and shall apply from the date of introducing the new VAT (regardless of the date when the Arrangement was signed).</td></tr>
<tr><td>5.3.2. Revision of the Contract Price/fees due to changes in other charges affecting changes in the Service price/fees</td><td colspan="2">Not applicable</td></tr>
<tr><td>5.3.3. Revision of the Contract Price/fees due</td><td colspan="2">5.3.3.1. During the term of the Contract, either Party to the Contract shall have the right to initiate a revision/change of the Contract</td></tr>
</table>

to changes in the price level	Price/fees not earlier than 6 months after the date of entry into force of the Contract (if the revision has already been carried out, from the date of the entry into force of the Arrangement on the last recalculation pursuant to this point of the Special Conditions) if 'J62 Computer programming, consultancy and related activities' price change (k) calculated following the procedure established in point 5.3.3.6 exceeds 5%. The revision of the Contract Price/fees shall be carried out at least every 6 months. 5.3.3.2. The Contract Price/fees shall be revised only for the part of the Contract that has not been redeemed, i.e. for the Services that have not been accepted and paid for. A subsequent revision of Contract Price/fees may not cover the period, for which the revision has already been carried out. 5.3.3.3. If the delay in provision of the Services is caused by the Provider, the price/rates of the Services provided with delay shall not be subject to recalculation due to price level increases (they can be reduced but not increased). 5.3.3.4. When revising the Contract Price/fees, the Parties shall be guided by the data from the Indicators Database published by the State Data Agency on the Official Statistics Portal. The other Party shall not be required to provide an official document or certification issued by the State Data Agency or other authority. 5.3.3.5. The Parties shall specify in the Arrangement the consumer products and services index value at the beginning of the period and the date of its determination, the index value at the end of the period and the date of its determination, the price change (k), the recalculated Contract Price/fees, and the recalculated Initial Contract Value. 5.3.3.6. The new Contract Price/fees shall be calculated according to the formula below: $a_1 = a + \left(\frac{k}{100} \times a\right)$, where a – price/fee (EUR, excluding VAT) (if the revision has already been carried out, then after the last recalculation) a_1 – recalculated (revised) price/fee (EUR, excluding VAT) k – change (increase or decrease) in the price for the (Services provided) (%) calculated according to (Prices of services) index 'J62 Computer programming, consultancy and related activities' . 'k' value shall be calculated according to the formula: $k = \frac{Ind_{naujausias}}{Ind_{pradžia}} \times 100 - 100(\%)$, where $Ind_{naujausias}$ – latest (Prices of services) index ('J62 Computer programming, consultancy and related activities') published on the date of sending the request for price/rate revision to the other Party). $Ind_{pradžia}$ – (Prices of services) index ('J62 Computer programming, consultancy and related activities') of the starting date (month) of the period. In case of the first recalculation, the starting date (month) of the period shall be the month of the date of entry into force of the Contract. In case of the second and subsequent recalculations, the beginning of the period (month) shall be the month of the published relevant index value used in the last recalculation.

<table>
<tr><td></td><td>5.3.3.7. The index values for calculations are used to four decimal places. The calculated change (k) used for further calculations is rounded to one decimal place, and the calculated fee a_1 is rounded to two decimal places.
5.3.3.8. A Party seeking a revision of the Contract Price/fees must apply in writing to the other Party and provide all necessary information in the request: title, number, date of the Contract, a list of the Services, which were not provided and not paid for, including quantities, Index values with references to public sources on the Official Statistics Portal of the State Data Agency or other official sources data, other important information proving a direct impact on the performance of the Contract and on the increase or decrease in the price of the Services. The Party shall not be entitled to specify a different Index in its request or to request a recalculation according to the different Index than specified in this procedure.
5.3.3.9. The Arrangement must be concluded within 20 working days from the date of receipt of a valid request submitted by the Party to recalculate the Contract Price/fees.
5.3.3.10. The Arrangement shall not entitle the Parties to modify the procedure set out in the Contract or any other provisions of the Contract, except where the modification is made in accordance with the provisions of the Law on Public Procurement.</td></tr>
<tr><td>5.3.4. Revision of the Contract price/fees due to changes in the price level according to price changes in the Service groups</td><td>Not applicable</td></tr>
<tr><td>5.4. Calculation of the Contract Price/fees by applying the rules for <u>quantity (volume)</u> change</td><td>Not applicable</td></tr>
<tr><td>5.5. Time limits and procedure of payment to the Provider</td><td>The Buyer shall pay to the Provider not later than within 30 calendar days from the date of receipt of the Invoice.

Conditions of payment:
Payment for the Services provided (Part I of the Procurement object - Implementation and configuration of VNA and DICOM based services (1 set) shall be made in phases after signing the Statement on the Transfer and Acceptance of the Services in the following order:
<table>
<tr><td>Completion of the initiation phase</td><td rowspan="3">20% of the price offered by the Provider</td></tr>
<tr><td>Completion of the detailed analysis phase</td></tr>
<tr><td>Completion of the design phase</td></tr>
<tr><td>Completion of the programming phase</td><td>20% of the price offered by the Provider</td></tr>
<tr><td>Completion of the deployment into the testing environment phase</td><td>40% of the price offered by the Provider</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Completion of the integration testing phase</td><td rowspan="2"></td></tr>
<tr><td>Completion of acceptance testing phase</td></tr>
<tr><td>Completion of training phase</td><td rowspan="4">20% of the price offered by the Provider</td></tr>
<tr><td>Completion of the deployment into the production environment</td></tr>
<tr><td>Completion of the trial operation phase</td></tr>
<tr><td>Signature of the final Statement on the Transfer and Acceptance of the Services and transfer of all project results</td></tr>
</table>
1) Payments for the completed Orders for additional development services (additional development hours) shall be made once a month.

Payments for the Support Services shall be made once a month (applicable only for Part I of the Procurement object)</td></tr>
<tr><td>5.6. Advance payment</td><td>Not applicable</td></tr>
<tr><td>5.7. Advance Security</td><td>Not applicable</td></tr>
<tr><td colspan="2">6. QUALITY OF THE SERVICES AND WARRANTY OBLIGATIONS</td></tr>
<tr><td>6.1. Warranty period</td><td>The Services shall be covered by the warranty during the period proposed by the Provider but, in any case, it should not be less than 12 months. The warranty period shall start from the day of signing the Statement on the Transfer and Acceptance of the Services or the Invoice (in case the Statement on the Transfer and Acceptance of the Services is not signed).</td></tr>
<tr><td>6.2. Deadline for elimination of defects in the Services</td><td>If defects in the Services are identified during the warranty period and/or at any time during the term of the Contract, the Provider shall remove them within the time limits specified in (6 section of the Technical Specification) of Annex No. 2 ‘Technical Specification’ to the Contract.</td></tr>
<tr><td>6.3. Procedures for the implementation and verification of qualitative criteria</td><td>The Buyer shall have the right to verify at any time during the performance of the Contract how the Provider complies with/ensures the implementation of the qualitative criteria conditions, for which the Provider has been awarded economic advantage points and, if necessary, shall have the right to ask the Provider to submit documents justifying the implementation of the qualitative criteria, which the Provider must submit not later than within 5 working days from the receipt of the Buyer’s request.</td></tr>
<tr><td colspan="2">7. SUB-PROVIDERS, ECONOMIC OPERATORS, SPECIALISTS USED FOR THE PERFORMANCE OF THE CONTRACT</td></tr>
<tr><td>7.1. The Provider shall use the following sub-providers for the performance of the Contract</td><td>No sub-providers shall be involved in the performance of the Contract</td></tr>
</table>

7.2. For the performance of the Contract, the Provider shall use the following **economic operators whose qualifications it relies on** to meet the qualification requirements set out in the Procurement documents.	Economic operators whose qualifications are relied on shall not be involved in the performance of the Contract
7.3. For the performance of the Contract, the Provider shall use the following **specialists whose qualifications it relies on** to meet the qualification requirements set out in the Procurement documents.	Specialists whose qualifications it relies on: Project Manager - Information system architect - Information system analyst - \ Backend developer - Frontend developer - Database developer Testing specialist - (Information system security specialis - |
7.4. For the performance of the Contract, the Provider shall use the following **specialists who earned the economic advantage points to the Provider** during the evaluation of the tender bid	Specialists who earned the economic advantage points to the Provider: Information systems architect - Backend programmer - Information systems analyst - Project manager -
7.5. The Provider shall use the following **specialists** for the performance of the Contract	-
8. SECURING THE DISCHARGE OF CONTRACTUAL OBLIGATIONS	
8.1. Securing the discharge of contractual obligations	The discharge of contractual obligations shall be secured by: 8.1.1. Penalty charges (default interest, fine);
8.2 Term of validity of the Performance Security	Not applicable
8.3. Submission of the Performance Security	Not applicable
9. LIABILITIES OF THE PARTIES	
9.1. Penalty charges for late payment under the Contract applicable to the Buyer	If the Buyer, having received a duly submitted and completed Invoice, delays payment for the good quality Services duly provided by the Provider within the time limit specified in the Contract, the Provider shall charge the Buyer a default interest in the amount of 0.05% of the outstanding amount, excluding VAT, for each day of delay, starting from the day after the due date.
9.2. Penalty charges applicable to the Provider	9.2.1. If the Provider is late in provision of the Services or fails to comply with other contractual obligations, the Buyer shall charge the Provider, starting from the day following the due date, a default interest in the amount of 0.05% of the price of the Services not provided on time, or

	of other contractual obligations not fulfilled, excluding VAT, for each day of delay. 9.2.2. The Provider shall be obliged to pay penalty charges to the Buyer within 30 calendar days from the Buyer's claim if the amount of penalty charges is not deducted from the amount due to the Provider. 9.2.3. For failure to comply with the deadline for elimination of errors and deficiencies identified in Annex 1 'Requirements for Procurement Object' to Annex 2 'Technical specification' to the Contract during the warranty period, the following fines shall be imposed: 9.2.3.1. In case of a critical error or deficiency: a fine of EUR 1 000.00 is imposed for each subsequent working day. 9.2.3.2. In case of a non-critical error or deficiency: a fine of EUR 100.00 is imposed for each subsequent working day. 9.2.4. For failure to comply with the response times set out in Annex 1 'Requirements for Procurement Object' to Annex 2 'Technical specification' to the Contract during the warranty period the following fines shall be imposed: 9.2.4.1. In case of a critical problem: a fine of EUR 100.00 is imposed for each additional hour. 9.2.4.2. In case of a non-critical problem: a fine of EUR 10.00 is imposed for each additional hour.
9.3. The Provider/Buyer shall be subject to a fine upon termination of the Contract due to the material breach thereof or upon unjustified termination of the performance of the Contract in conflict to the procedure laid down therein	9.3.1. In the event of termination of the Contract due to the material breach thereof, as set out in the Special Conditions of the Contract, a fine in the amount of 10% of the Initial Contract Value as set out in point 5.2 of the Special Conditions shall be paid. 9.3.2. In the event of unjustified termination of the performance of the Contract in conflict to the procedure laid down therein, a fine in the amount of 10% of the Initial Contract Value as set out in point 5.2 of the Special Conditions shall be paid.
9.4. Fine applicable to the Provider for replacing the existing sub-providers or specialists/using new sub-providers in conflict to the procedure for replacing sub-providers and/or specialists set out in the General Conditions	If the Provider changes the person specified in points 7.1-7.5 in conflict to the procedure for changing sub-providers and/or specialists provided for in the General Conditions, a fine of EUR 1 000.00 shall be paid on a case-by-case basis.
9.5. Fines applicable to the Provider for non-compliance with environmental and/or social criteria	Not applicable
9.6. Fine applicable to the Provider/Buyer for non-compliance with	If the Provider/Buyer fails to comply with the confidentiality requirements specified in the General Conditions, a fine of EUR 10 000.00 shall be paid.

confidentiality requirements	
9.7. Penalty charges applicable to the Provider for failure to meet the qualitative criteria set out in the Procurement documents during the performance of the Contract	If the Provider does not ensure compliance with the qualitative criteria set out in the Procurement documents (or does not reach it (them)) during the term of the Contract, for which the Provider has been awarded economic advantage points, the following fine shall be paid: 1. For Criterion '**Additional experience of the information systems architect proposed by the service provider**' – 2.33% of value of the Services not provided. 2. For Criterion **'Additional experience of the backend programmer proposed by the service provider' –** 2.33% of value of the Services not provided. 3. For Criterion '**Additional experience of the information systems analyst proposed by the service provider' –** 2.33% of value of the Services not provided. 4.For Criterion '**Additional experience of the Project manager proposed by the service provider**' – 2.33% of value of the Services not provided.
9.8. Penalty charges applicable to the Provider for failure to renew the Performance Security	Not applicable
9.9. The Provider shall be subject to a fine for non-compliance with the requirements for the use of Buyer's symbols, name and brand in advertising or marketing and prohibition to use results of intellectual activity produced by the Buyer	5% of the Initial Contract Value specified in point 5.2 of the Special Conditions.
9.10. Other penalty charges and civil liability of the Parties to the Contract	**Other penalty charges:** 9.10.1. If the specialist referred to in Section 7 of the Special Conditions does not attend a pre-planned (not later than 2 working days) meeting where their participation, to the opinion of the Buyer, is required and there are no objective reasons for their non-attendance (such as sick leave, etc.), the Provider shall pay a fine of EUR 500.00 (five hundred). 9.10.2. If the Provider is late in providing the Services within the time limits set in the Project implementation schedule, the Buyer shall charge the Provider a default interest in the amount of 0.05% of the price for the Services not provided in time or other contractual obligations not discharged, excluding VAT, for each day of delay, starting from the day after the due date.
10. ESSENTIAL TERMS OF THE CONTRACT	
10.1. Essential terms of the Contract	Obligations specified in point 12.2. of the Special Conditions, non-compliance with which shall be considered a material breach.
11. VALIDITY AND AMENDMENT OF THE CONTRACT	

11.1. Conclusion and entry into force of the Contract	This Contract shall be deemed to have been concluded and shall enter into force on the date of signing of the Contract (date of signature of the other Party). The Contract shall be valid until full discharge of obligations (until the Initial Contract Value is fully used; however, its term cannot be longer than - *86 months* (including all possible extensions of the Service provision and time limit for the provision of the Services as well as time limits for payment for the Services)).
11.2. Extension of the Contract validity period	Not applicable
12. TERMINATION OF THE CONTRACT	
12.1. Grounds for termination of the Contract	The Contract may be terminated by written agreement of the Parties or unilaterally, in accordance with the procedure laid down in the General Conditions.
12.2. Material breaches of the Contract	12.2.1. If the Provider fails to meet its obligations for the Contract price/fees set out in the Contract. 12.2.2. If the Provider fails to provide an extension of the Performance Security for more than 30 days after expiry of the Performance Security validity period in accordance with the procedures set out in the General Conditions (except for the original Performance Guarantee) (**this provision shall be applicable where performance of the Contract is guaranteed by means other than those referred to in point 8.1.1 of the Contract**). 12.2.3. If it turns out that the Provider fails to fulfil the obligations that were established in the Procurement documents as tender bid evaluation criteria during the tender bid evaluation and for which the Provider was awarded points, when the tender bid was evaluated on the price/cost and quality ratio, and the Provider does not correct violations within 10 calendar days (**this provision shall be applicable when the tender bid is evaluated on the price/cost-quality ratio**). 12.2.4. If the Provider fails to meet time limits for provision of the Services set out in the Contract on 2 (two) consecutive occasions, or provision of the Services is delayed for longer than 20 days from the deadline for provision of the Services set out in the Contract. 12.2.5. If the Provider violates time limits for the provision of the Services and the amount of penalty charges for the delay exceeds 20% of the Initial Contract Value. 12.2.6. The Provider violates time limits for provision of the Services, and delay in the provision of the Services renders their provision unnecessary. 12.2.7. The Provider provides the Services that do not comply with the requirements for the Services set out in the Contract and/or the Laws on more than 2 occasions. 12.2.8. The Provider's qualifications no longer meet the requirements laid down in the Procurement documents for the proper performance of the Contract, and the non-compliance has not been rectified within 10 working days from the date on which the qualifications became non-compliant (**this provision shall be applicable where the**

	Procurement documents have laid down the requirements for the qualification of tenderers). 12.2.9. The Provider is in breach of the provisions of this Contract governing competition, intellectual property or the management of confidential information. 12.2.10. The Provider is in breach of the provisions of the General Conditions regarding the use of new sub-providers and/or specialists for the performance of the Contract/replacement of existing sub-providers and/or specialists. 12.2.11. The Provider and/or a joint venture partner (if applicable) and/or sub-provider (if applicable), at the time of provision of the Services, for which the requirements of the environmental management system are established in the Contract, does not have a valid environmental management system certificate and/or does not provide an extension of the certificate(does not acquire a new one) **(this provision shall be applicable when the requirements of the environmental management system have been established in the Procurement documents).** 12.2.12. The Provider 2 (two) times violates the essential condition of the Contract. 12.2.13. It became apparent that the Provider should not have been awarded the Contract because the Court of Justice of the European Union, in proceedings pursuant to Article 258 of the Treaty on the Functioning of the European Union, has found that the obligations under the Treaties establishing the European Union and Directive 2014/24/EU have not been met. 12.2.14. The Government of the Republic of Lithuania, in accordance with the procedure established by the Law on the Protection of Objects of Importance to Ensuring National Security, adopts a decision confirming that the Contract (or an amendment thereto) is considered to pose a risk or fails to conform to the national security interests. 12.2.15. The Contract was amended in breach of Article 89 of the Law on Public Procurement. 12.2.16. It became apparent that the Provider who was awarded the Contract should have been excluded from the Procurement procedure in accordance with Article 46(1) of the Law on Public Procurement. 12.2.17. The circumstances referred to in Articles 37(9), 45(2^1) and/or 4 (9) of the Law on Public Procurement have been identified.
13. ENVIRONMENTAL AND SOCIAL CRITERIA	
13.1. Environmental criteria related to the Services procured	Not applicable
13.2. Social criteria related to the Services procured	Not applicable
14. AMENDMENTS AND SUPPLEMENTS TO THE GENERAL CONDITIONS	

14.1.	The Parties shall agree to amend **point 1.3.1** of the General Conditions of the Contract and recast it as follows: '1.3.1. The documents constituting the Contract shall be understood as complementing each other. In the event of any inconsistency or ambiguity in the conditions of the Contract documents, such inconsistency or ambiguity shall be eliminated by interpreting the documents in the following order of priority: 1.3.1.1. Special Conditions 1.3.1.2. Technical Specification 1.3.1.3. General Conditions 1.3.1.4. Procurement documents (except for Technical Specification) 1.3.1.5. Tender bid 1.3.1.6. Other annexes listed in Special Conditions'
14.2.	Alternative provisions (marked 'if applicable', etc.) referred to in the General Conditions of the Contract shall only apply if they are specifically described in the Special Conditions of the Contract.
14.3.	The Parties shall agree to add the following point to the General Conditions of the Contract but not to change the numbering of the other points: '17.7. The Provider is advised to comply with the provisions of the Code of Conduct for Tenderers issued by the Public Procurement Office[1] . The Provider undertakes to ensure compliance with the provisions of points 35-37 of the Code of Conduct for Tenderers throughout the term of validity of the Contract.'
14.4.	In the event of a proposal received from the Commission for Coordination of the Protection of Objects of Importance for National Security, the Parties shall agree to supplement the General Conditions of the Contract with the above-mentioned point but not to change the numbering of other points: '16.5. The Provider undertakes not to provide any information to entities of the Russian Federation, the Republic of Belarus, the People's Republic of China (or persons representing them) and to ensure that entities of these countries are not used to participate in this Contract in any form.' Or indicate another proposal of the Commission for Coordination of Protection of Objects Critical for National Security.
14.5.	The Parties shall agree to amend point 17.2. of the General Conditions of the Contract and recast it as follows: '17.2. Payment of penalty charges and/or the receipt of the Performance Security shall not deprive the Party of the right to demand the other Party to compensate for the direct losses or damage as well as additional expenditure incurred by it. The penalty charges provided for in this Contract shall be deemed to be minimal losses of the Parties that do not need to be justified. Each of the Parties shall be entitled to receive indemnity from the other Party for the improper performance or non-performance of contractual obligations of the other Party, up to the Initial Contract Value, unless the legislation provides for a higher amount to be reimbursed. The limitation of liability provided for in this point shall not apply if the damage is caused by breach of confidentiality

[1] Code of Conduct for Tenderers developed by the Public Procurement Office https://vpt.lrv.lt/media/viesa/saugykla/2024/1/w2fscibRf-4.pdf

	obligations, personal data protection legislation or intellectual property rights.'
14.6.	The Parties shall agree to add the following point to the General Conditions of the Contract but not to change the numbering of the other points: '3.2.15. The Customer shall not verify the compliance of specialists with the qualification requirements set out in the Procurement documents if additional specialists specified in point 7.5 of the Special Conditions of the Contract are involved.'
15. ANNEXES TO THE CONTRACT	
15.1. Annex No. 1	General Conditions
15.2. Annex No. 2	Technical Specification
15.3. Annex No. 3	Tender Bid
15.4. Annex No. 4	Form of the Statement of Transfer and Acceptance of the Services
15.7. Annex No. 5	Defect Report
15.5. Annex No. 6	Agreement on the processing of personal data
15.6. Annex No. 7	Arrangement on applicable organisational and technical cybersecurity requirements
16. SIGNATURES OF REPRESENTATIVES OF THE PARTIES	
BUYER	**PROVIDER:**
Director General,	CEO,
(Signature)	**(Signature)**

Special Part of the Contract for the Public Procurement-Sale of Services No. ST-
Annex No. 4

(Template of the Statement on the Transfer and Acceptance)

Statement on the Transfer and Acceptance of the SERVICES

No

_____
(place of creation)

The responsible persons who signed this Statement confirm that in accordance with the signed (insert title and number of the Contract) (hereinafter referred to as the Contract), the Provider transfers and the Buyer accepts the Services specified in the Table below:

No	Name of service	Activity code*	Measurement unit	Quantity	Unit price, in EUR, excluding VAT	Amount, in EUR, excluding VAT
1.		Choose				
2.		Choose				
3.		Choose				
					Total:	
					VAT (specify) %:	
					Total amount:	

** Activity code is agreed with the Buyer.*

The Provider has provided all Services and submitted all necessary documents under the Contract
Please select

SERVICES ACCEPTED BY:
State Enterprise Centre of Registers

_____
(position of the responsible person)
(name and surname)

SERVICES PROVIDED BY:
(Name of the Provider):

_____
(position of the responsible person)
(name and surname)

(Template of Defect Report)

DEFECT REPORT
No

_____
(place of creation)

We note that pursuant to the signed (enter title of the Contract and No.) (hereinafter referred to as the Contract) the Buyer has identified the defects of the Services and/or products related to the Services and/or documents provided by the Provider in the following table:

No	Description of defects in the Services /products related to the Services/documents	Procedure for elimination of defects	Deadline for elimination of defects
1.			
2.			
3.			
...			

_____	_____	_____
(Position of the person responsible for the performance of the Contract)	(Signature)	(Name and surname)

PASLAUGŲ PIRKIMO-PARDAVIMO SUTARTIES SPECIALIOSIOS SĄLYGOS

Sutarties pavadinimas	I pirkimo objekto dalis - DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas	
1. SUTARTIES ŠALYS		
1.1. Pirkėjas	1.1.1. Pavadinimas	Valstybės įmonė Registrų centras
	1.1.2. Juridinio asmens kodas	124110246
	1.1.3. Adresas	Studentų g. 39, LT-08106 Vilnius
	1.1.4. PVM mokėtojo kodas	LT241102419
	1.1.5. Atsiskaitomoji sąskaita	LT94 4010 0424 0005 0387
	1.1.6. Depozitinė banko sąskaita	LT14 7300 0101 3363 7868
	1.1.7 Bankas, banko kodas	Luminor Bank AS Lietuvos skyrius, banko kodas 40100
	1.1.8. Telefonas	+370 5 268 8262
	1.1.9. El. paštas	info@registrucentras.lt
	1.1.10. Šalies atstovas	Generalinis direktorius Adrijus Jusas
	1.1.11. Atstovavimo pagrindas	Imonės įstatai
1.2. Tiekėjas	1.2.1. Pavadinimas	J4Care, GmbH
	1.2.2. Juridinio asmens kodas	Commercial Register Number: FN 298641d
	1.2.3. Adresas	Enzersdorferstraße 7 2340 Mödling, Austria
	1.2.4. PVM mokėtojo kodas	ATU 63646825
	1.2.5. Atsiskaitomoji sąskaita	IBAN 124300033643870000
	1.2.6. Bankas, banko kodas	Volksbank Wien Bank code:43000
	1.2.7. Telefonas	+
	1.2.8. El. paštas	
	1.2.9. Šalies atstovas	
	1.2.10. Atstovavimo pagrindas	CEO
2. ATSAKINGI ASMENYS		
2.1. Pirkėjo kontaktiniai asmenys, atsakingi už Sutarties vykdymą, Paslaugų priėmimą, Sąskaitų per informacinę sistemą SABIS priėmimą		

2.2. Tiekėjo kontaktiniai asmenys, atsakingi už Sutarties vykdymą	
3. SUTARTIES DALYKAS	
3.1. Sutarties dalykas	Tiekėjas įsipareigoja Sutartyje numatytomis sąlygomis suteikti Pirkėjui Paslaugas - DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas; Išsamus Paslaugų aprašymas ir kiti reikalavimai teikiamoms Paslaugoms nustatyti Sutarties priede Nr. 2 „Techninė specifikacija" (toliau – Techninė specifikacija) ir Sutarties priede Nr. 3 „Pasiūlymas".
3.2. Pirkimo pavadinimas ir numeris	Kompleksinio MedVAIS modernizavimo sprendimo pirkimas ir įdiegimas. CVP IS Nr. 2254548
3.3. Informacija apie Europos Sąjungos lėšomis finansuojamą projektą arba kitą projektą	Europos Sąjungos lėšomis bendrai finansuojamo projekto Nr. 09-033-P-0001 „Nacionalinės medicininių vaizdų archyvavimo ir mainų sistemos ir jos teikiamų elektroninių paslaugų plėtra" (toliau – Projektas).
4. PASLAUGŲ SUTEIKIMO TERMINAI IR PASLAUGŲ PERDAVIMO – PRIĖMIMO TVARKA	
4.1. Paslaugų suteikimo terminas, kai Paslaugos yra vienkartinio pobūdžio, teikiamos periodiškai arba pagal Pirkėjo Užsakymą	4.1.1.Tiekėjas Paslaugas DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas (toliau – Paslaugos), Papildomai užsakomos vystymo paslaugos (toliau – papildomos paslaugos), Sistemos priežiūros paslaugos (toliau – priežiūros paslaugos), Papildomai užsakomos vystymo paslaugos (toliau – papildomos paslaugos)), įsipareigoja suteikti **ne vėliau kaip per 7 mėnesius** nuo Sutarties įsigaliojimo dienos (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę ne mažiau kaip 7 mėnesiai) **arba iki 2026-04-30** (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę mažiau kaip 7 mėnesiai). 4.1.2. Tiekėjas papildomas vystymo Paslaugas įsipareigoja teikti nuo Sutarties įsigaliojimo dienos 7 mėnesius (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę ne mažiau kaip 7 mėnesiai) arba iki 2026-04-30 (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę mažiau kaip 7 mėnesiai). Paslaugų Užsakymai gali būti teikiami ir turi būti įvykdyti per Užsakyme nurodytą terminą, tačiau ne vėliau, nei iki aukščiau nurodyto termino pabaigos / datos. 4.1.3. Priežiūros paslaugos turės būti teikiamos (jei jos bus užsakytos) užsakytą laikotarpį, bet ne ilgiau kaip 60 mėnesių. Priežiūros paslaugos pradedamos teikti ne anksčiau nei pasibaigs garantinės priežiūros laikotarpis ir gavus Perkančiosios organizacijos užsakymą. (Taikoma tik I p.o.d.)
4.2. Paslaugų / jų dalies / etapo / periodo suteikimo	4.2.1. Sutarties šalys turi teisę į Paslaugų suteikimo termino nurodyto 4.1.1. punkte pratęsimą, tačiau tik tuo atveju, jei: 4.2.1.1. atsiranda įrodymais pagrįstų kliūčių ar trukdymų, kurių atsiradimui Sutarties šalys neturi įtakos ir už kuriuos jos neatsako, ir kurie sukelti ir priskirtini tretiesiems asmenims, ar kitų aplinkybių, kurių Sutarties šalys

<table>
<tr><td>termino pratęsimas</td><td colspan="2">negalėjo iš anksto numatyti. Aplinkybės, kuriomis grindžiama būtinybė pratęsti Paslaugų suteikimo terminą, jokiu būdu negali priklausyti nuo Sutarties šalių. Kiekvienu tokiu atveju, Sutarties šalis, inicijuojanti Paslaugų suteikimo termino pratęsimą, raštu nedelsdama, bet ne vėliau kaip per 5 darbo dienas, apie tai praneša kitai Sutarties šaliai, pateikdama minėtų aplinkybių egzistavimo įrodymus. Nurodytas aplinkybes vertina kita Sutarties šalis, šiai sutikus, Paslaugų suteikimo terminas gali būti pratęsiamas tik minėtų aplinkybių egzistavimo laikotarpiui, tačiau ne ilgiau kaip:
4.2.1.1.1. iki 2026-04-30;
arba
4.2.1.1.2. Projekto įgyvendinimo terminui, jei Projekto įgyvendinimo terminas bus pratęstas, tačiau ne ilgiau, kaip <u>6 mėnesių</u> laikotarpiui;
arba
4.2.1.1.3. ne ilgesniam, kaip 6 mėnesių laikotarpiui tuo atveju, jei bus skirtas finansavimas ne iš Projekto lėšų.

4.2.2. Papildomų vystymo Paslaugų teikimo terminas, nurodytas Specialiųjų sąlygų 4.1.2. punkte, gali būti pratęstas jei nebus išnaudota Specialiųjų sąlygų 5.2 p. nurodyta Pradinė Sutarties vertė. Tokiu atveju, Pirkėjas raštu apie tai praneša Tiekėjui, nurodydamas kokiam terminui siūloma pratęsti Paslaugų teikimo terminą. Tiekėjui sutikus, Paslaugų teikimo terminas gali būti pratęsiamas tik kol bus išnaudota Specialiųjų sąlygų 5.2 p. nurodyta Pradinės Sutarties vertė, bet ne ilgiau nei 6 mėnesių laikotarpiui (pratęsimų kiekis neribojamas).</td></tr>
<tr><td>4.3. Užsakymų teikimo tvarka</td><td colspan="2">Papildomų paslaugų užsakymų teikimo tvarka aprašyta Techninės specifikacijos pirmame priede "Reikalavimai pirkimo objektui" 6.2. skyriuje "Reikalavimai paslaugų užsakymui".</td></tr>
<tr><td>4.4. Dėl minimalios Užsakymo vertės ar apimties</td><td colspan="2">Netaikoma</td></tr>
<tr><td rowspan="6">4.5. Pateikiami dokumentai</td><td colspan="2">Turi būti pateikiami šie dokumentai (Tiekėjui nepateikus nurodytų dokumentų, laikoma, kad Paslaugos neatitinka Sutartyje nustatytų reikalavimų):</td></tr>
<tr><td>4.5.1. Paslaugų perdavimo–priėmimo aktas</td><td>Taip</td></tr>
<tr><td>4.5.2. Sąskaita</td><td>Taip</td></tr>
<tr><td>4.5.3. Sutarties priedo Nr. 2 „Techninė specifikacija“ nurodyti dokumentai</td><td>Taip</td></tr>
<tr><td>4.5.4. Sutarties priedo Nr. 2 „Techninė specifikacija“, 1 priedo „Reikalavimai pirkimo objektui“ nurodyti dokumentai</td><td>Taip</td></tr>
<tr><td colspan="2">Tiekėjui nepateikus nurodytų dokumentų, laikoma, kad Paslaugos neatitinka Sutartyje nustatytų reikalavimų.</td></tr>
<tr><td colspan="3">5. SUTARTIES KAINA IR ATSISKAITYMO TVARKA</td></tr>
<tr><td>5.1. Sutarčiai taikomas kainos apskaičiavimo būdas</td><td colspan="2">Mišri kainodara (fiksuotos kainos ir fiksuoto įkainio)</td></tr>
</table>

<table>
<tr><td>5.2. Pradinės Sutarties vertė ir Sutarties kaina</td><td colspan="2">Pradinės Sutarties vertė yra 3.980.000,00 Eur, be pridėtinės vertės mokesčio (toliau – PVM).
PVM sudaro 835.800,00 Eur.
Sutarties kaina yra 4.815.800,00 Eur su PVM.
Šioje Sutartyje Pradinės Sutarties vertė yra lygi maksimaliai pirkimui skirtai lėšų sumai be PVM pirkimo dokumentuose ir Sutartyje nurodytų Paslaugų įsigijimui:
5.2.1. Paslaugų suteikimo kaina ((DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas, paslaugos (1 kompl.) yra lygi Tiekėjo pasiūlymo kainai be PVM, nurodytai už visą pirkimo dokumentuose ir Sutartyje nurodytą Paslaugų kiekį ir (ar) apimtį (fiksuotos kainos kainodara);
5.2.2. Papildomos vystymo Paslaugos yra įsigyjamos Tiekėjo pasiūlyme nurodytais įkainiais be PVM. Pirkėjas perka papildomas vystymo Paslaugas pagal poreikį Sutartyje arba jos priede 3 „Pasiūlymas“ nurodytais įkainiais, neviršijant Sutarties kainos. Sutartyje arba jos priede Nr. 3 „Pasiūlymas“ nurodytas papildomų vystymo Paslaugų kiekis yra maksimalus. Pirkėjas neįsipareigoja išpirkti maksimalaus papildomų vystymo Paslaugų kiekio ar bet kokios jo dalies (fiksuoto įkainio kainodara).
5.2.3. Pirkėjas užsakys priežiūros paslaugas tik tuo atveju, jei bus gautas finansavimas šių paslaugų įsigijimui. Paslaugos bus užsakomos atsižvelgiant į faktiškai gauto finansavimo dydį ir apmokamos Sutartyje arba jos 3 priede „Pasiūlymas“ nustatytais įkainiais, neviršijant bendros Sutarties kainos. Pirkėjas neįsipareigoja užsakyti viso pasiūlyto priežiūros paslaugų kiekio ar jo dalies. Taikoma fiksuoto įkainio kainodara.</td></tr>
<tr><td rowspan="5">5.3. Sutarties kainos / įkainių perskaičiavimas taikant <u>peržiūros</u> taisykles</td><td colspan="2">Sutarties kaina / įkainiai bus perskaičiuojami:</td></tr>
<tr><td>5.3.1. dėl PVM tarifo pasikeitimo</td><td>Taip</td></tr>
<tr><td>5.3.2. dėl kitų mokesčių, lemiančių Paslaugų kainos pokytį, pasikeitimo</td><td>Ne</td></tr>
<tr><td>5.3.3. dėl kainų lygio pokyčio</td><td>Taip</td></tr>
<tr><td>5.3.4. pagal Paslaugų grupių kainų pokyčius</td><td>Ne</td></tr>
<tr><td>5.3.1. Sutarties kainos / įkainių peržiūra dėl PVM tarifo pasikeitimo</td><td colspan="2">Jeigu Sutarties vykdymo metu pasikeičia PVM mokėjimą reglamentuojantys teisės aktai, darantys tiesioginę įtaką Tiekėjo teikiamų Paslaugų Sutartyje nurodytai kainai / įkainiams, Sutarties kaina / įkainiai perskaičiuojami nekeičiant Paslaugų kainos / įkainio be PVM.

Perskaičiuota (-i) Sutarties kaina / įkainiai įforminama (-i) Susitarimu ir turi būti taikoma (-i) nuo naujo PVM įvedimo datos (nepriklausomai nuo to, kada pasirašytas Susitarimas).</td></tr>
<tr><td>5.3.2. Sutarties kainos / įkainių peržiūra dėl kitų mokesčių, lemiančių Paslaugų kainos / įkainių pokytį, pasikeitimo</td><td colspan="2">Netaikoma</td></tr>
<tr><td>5.3.3. Sutarties kainos / įkainių</td><td colspan="2">5.3.3.1. Bet kuri Sutarties Šalis Sutarties galiojimo metu turi teisę inicijuoti Sutarties kainos / įkainių peržiūrą (keitimą) ne anksčiau kaip po 6 mėnesių</td></tr>
</table>

peržiūra dėl kainų lygio pokyčio	nuo Sutarties įsigaliojimo dienos (jeigu peržiūra jau buvo atlikta – nuo Susitarimo dėl paskutinio perskaičiavimo pagal šį Specialiųjų sąlygų punktą įsigaliojimo dienos), jeigu („J62 Kompiuterių programavimo, konsultacinė ir susijusi veikla“) kainų pokytis (k), apskaičiuotas kaip nustatyta 5.3.3.6 punkte, viršija 5 procentus. Sutarties kainos / įkainių peržiūra atliekama ne rečiau kaip kas 6 mėnesius. 5.3.3.2. Sutarties kaina / įkainiai peržiūrimi tik tai Sutarties daliai, kuri nėra išpirkta, t. y. Paslaugoms, kurios nėra priimtos ir apmokėtos. Vėlesnė Sutarties kainos / įkainių peržiūra negali apimti laikotarpio, už kurį jau buvo atlikta peržiūra. 5.3.3.3. Jeigu Paslaugų teikimas vėluoja dėl Tiekėjo kaltės, uždelstų suteikti Paslaugų kaina / įkainiai nėra perskaičiuojami dėl kainų lygio kilimo (gali būti mažinami, tačiau negali būti didinami). 5.3.3.4. Atlikdamos Sutarties kainos / įkainių peržiūrą Šalys vadovaujasi Valstybės duomenų agentūros viešai Oficialiosios statistikos portale paskelbtais Rodiklių duomenų bazės duomenimis. Iš kitos Šalies nereikalaujama pateikti oficialaus Valstybės duomenų agentūros ar kitos institucijos išduoto dokumento ar patvirtinimo. 5.3.3.5. Šalys privalo Susitarime nurodyti vartojimo prekių ir paslaugų indekso reikšmę laikotarpio pradžioje ir jo nustatymo datą, indekso reikšmę laikotarpio pabaigoje ir jo nustatymo datą, kainų pokytį (k), perskaičiuotą Sutarties kainą / įkainius, perskaičiuotą Pradinės Sutarties vertę. 5.3.3.6. Nauja Sutarties kaina / įkainiai apskaičiuojami pagal žemiau pateiktą formulę: $a_1 = a + \left(\frac{k}{100} \times a\right)$, kur a – kaina / įkainis (Eur be PVM) (jei peržiūra jau buvo atlikta, tai po paskutinio perskaičiavimo) a_1 – perskaičiuota (pakeista) kaina / įkainis (Eur be PVM) k – pagal (Paslaugų kainų) indeksą („J62 Kompiuterių programavimo, konsultacinė ir susijusi veikla“) apskaičiuotas (suteiktų paslaugų) kainų pokytis (padidėjimas arba sumažėjimas) (%). „k“ reikšmė skaičiuojama pagal formulę: $k = \frac{\mathrm{Ind}_{\mathrm{naujausias}}}{\mathrm{Ind}_{\mathrm{pradžia}}} \times 100 - 100$, (proc.) kur $\mathrm{Ind}_{\mathrm{naujausias}}$ – kreipimosi dėl kainos / įkainių peržiūros išsiuntimo kitai Šaliai dieną paskelbtas naujausias (Paslaugų kainų) indeksas („J62 Kompiuterių programavimo, konsultacinė ir susijusi veikla“). $\mathrm{Ind}_{\mathrm{pradžia}}$ – laikotarpio pradžios datos (mėnesio) (Paslaugų kainų) indeksas („J62 Kompiuterių programavimo, konsultacinė ir susijusi veikla“). Pirmojo perskaičiavimo atveju laikotarpio pradžia (mėnuo) yra Sutarties įsigaliojimo dienos mėnuo. Antrojo ir vėlesnių perskaičiavimų atveju laikotarpio pradžia (mėnuo) yra paskutinio perskaičiavimo metu naudotos paskelbto atitinkamo indekso reikšmės mėnuo. 5.3.3.7. Skaičiavimams indeksų reikšmės imamos **keturių** skaitmenų po kablelio tikslumu. Apskaičiuotas pokytis (k) tolimesniems skaičiavimams naudojamas suapvalinus iki **vieno** skaitmens po kablelio, o apskaičiuotas įkainis „a_1“ suapvalinamas iki **dviejų** skaitmenų po kablelio. 5.3.3.8. Šalis, siekianti Sutarties kainos / įkainių peržiūros, privalo raštu kreiptis į kitą Šalį ir prašyme pateikti visą reikalingą informaciją: Sutarties pavadinimą, numerį, datą, neperduotų ir neapmokėtų Paslaugų sąrašą su kiekiais, indekso reikšmes su nuorodomis į viešus šaltinius Valstybės duomenų

<table>
<tr><td></td><td>agentūros Oficialiosios statistikos portale arba kitus oficialius šaltinių duomenis, kita svarbi informacija įrodanti tiesioginę įtaką Sutarties vykdymui ir Paslaugų kainos didėjimui ar mažėjimui. Prašyme Šalis neturi teisės nurodyti kito indekso ar prašyti perskaičiavimo pagal kitą indeksą nei nurodytas šioje procedūroje.
5.3.3.9. Susitarimas turi būti sudarytas per 20 darbo dienų nuo Šalies pateikto tinkamo prašymo perskaičiuoti Sutarties kainą / įkainius gavimo dienos.
5.3.3.10. Susitarimu Šalys neturi teisės keisti procedūroje nurodytos tvarkos ar kitų Sutarties nuostatų, išskyrus, jei keitimas atliekamas pagal VPĮ nuostatas.</td></tr>
<tr><td>5.3.4. Sutarties kainos / įkainių peržiūra dėl kainų lygio pokyčio pagal Paslaugų grupių kainų pokyčius</td><td>Netaikoma</td></tr>
<tr><td>5.4. Sutarties kainos / įkainių apskaičiavimas taikant <u>kiekio (apimties)</u> keitimo taisykles</td><td>Netaikoma</td></tr>
<tr><td>5.5. Atsiskaitymo su Tiekėju terminas ir tvarka</td><td>Pirkėjas atsiskaito su Tiekėju ne vėliau kaip per 30 kalendorinių dienų nuo Sąskaitos gavimo dienos.

Apmokėjimo sąlygos:
už suteiktas Paslaugas (DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas, paslaugos (1 kompl.) atsiskaitoma etapais pasirašius Paslaugų perdavimo-priėmimo aktą, tokia tvarka:
<table>
<tr><td>Inicijavimo etapas baigtas</td><td rowspan="3">20 proc. Tiekėjo pasiūlytos kainos</td></tr>
<tr><td>Detalios analizės etapas baigtas</td></tr>
<tr><td>Projektavimo etapas baigtas</td></tr>
<tr><td>Programavimo etapas baigtas</td><td>20 proc. Tiekėjo pasiūlytos kainos</td></tr>
<tr><td>Diegimo į testavimo aplinką etapas baigtas</td><td rowspan="3">40 proc. Tiekėjo pasiūlytos kainos</td></tr>
<tr><td>Integracinio testavimo etapas baigtas</td></tr>
<tr><td>Priėmimo testavimo etapas baigtas</td></tr>
<tr><td>Mokymo etapas baigtas</td><td rowspan="3">20 proc. Tiekėjo pasiūlytos kainos</td></tr>
<tr><td>Diegimas į gamybinę aplinką etapą baigtas</td></tr>
<tr><td>Bandomosios eksploatacijos etapas baigtas</td></tr>
</table></td></tr>
</table>

	Pasirašomas galutinis Priėmimo – perdavimo aktas ir perduodami visi projekto rezultatai 1) už įvykdytus papildomų vystymo Paslaugų (papildomos vystymo valandos) Užsakymus mokama kartą per mėnesį. 2) už Priežiūros paslaugas mokama kartą per mėnesį.
5.6. Avansas	Netaikoma
5.7. Avanso užtikrinimas	Netaikoma
6. PASLAUGŲ KOKYBĖ IR GARANTINIAI ĮSIPAREIGOJIMAI	
6.1. Garantinis terminas	**Paslaugoms nustatomas** 12 mėn. garantinis terminas. Garantinis terminas skaičiuojamas nuo Paslaugų perdavimo–priėmimo akto ar Sąskaitos (kai Paslaugų perdavimo–priėmimo aktas nėra pasirašomas) pasirašymo dienos. Garantinis terminas skaičiuojamas nuo paskutinio Paslaugų arba papildomų vystymo Paslaugų (priklausomai nuo to kuris iš jų yra paskutinis) perdavimo–priėmimo akto ar Sąskaitos (kai Paslaugų perdavimo–priėmimo aktas nėra pasirašomas) pasirašymo dienos.
6.2. Terminas Paslaugų trūkumams pašalinti	Garantinio termino laikotarpiu ir (arba) bet kuriuo Sutarties galiojimo metu nustačius Paslaugų trūkumų, Tiekėjas turi juos pašalinti per Sutarties priede Nr. 2 „Techninė specifikacija", 6 skyriuje arba Defektų akte nurodytą terminą.
6.3. Kokybinių kriterijų įgyvendinimo ir tikrinimo tvarka	Pirkėjas bet kuriuo Sutarties vykdymo metu turi teisę tikrinti kaip Tiekėjas laikosi / užtikrina kokybinių kriterijų sąlygų įgyvendinimą, už kuriuos Tiekėjui buvo suteikti ekonominio naudingumo balai ir, esant poreikiui, turi teisę paprašyti Tiekėjo pateikti kokybinių kriterijų sąlygų įgyvendinimą pagrindžiančius dokumentus, kuriuos Tiekėjas privalo pateikti ne vėliau, kaip per 5 darbo dienas nuo Pirkėjo prašymo gavimo dienos.
7. SUTARTIES VYKDYMUI PASITELKIAMI SUBTIEKĖJAI, ŪKIO SUBJEKTAI, SPECIALISTAI	
7.1. Sutarties vykdymui Tiekėjas pasitelkia šiuos **subtiekėjus**	Sutarties vykdymui subtiekėjai nepasitelkiami
7.2. Sutarties vykdymui Tiekėjas pasitelkia šiuos **ūkio subjektus, kurių kvalifikacija remiasi**, kad atitiktų Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus.	Sutarties vykdymui ūkio subjektai, kurių kvalifikacija remiamasi, nepasitelkiami
7.3. Sutarties vykdymui Tiekėjas pasitelkia šiuos **specialistus, kurių kvalifikacija remiasi**, kad atitiktų Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus	Sutarties vykdymui specialistai, kurių kvalifikacija remiamasi: Projektų vadovas - IS architektas - IS analitikas - Backend programuotojas - Frontend programuotojas - Duomenų bazių programuotojas - Testuotojas -

	IS saugos specialistas -
7.4. Sutarties vykdymui Tiekėjas pasitelkia šiuos **specialistus, už kuriuos** pasiūlymo vertinimo metu **Tiekėjui buvo suteikti ekonominio naudingumo balai**	Sutarties vykdymui specialistai, už kuriuos pasiūlymo vertinimo metu Tiekėjui buvo suteikti ekonominio naudingumo balai: IS architektas - Backend programuotojas - IS analitikas - Projektų vadovas -
7.5. Sutarties vykdymui Tiekėjas pasitelkia šiuos **specialistus**	Sutarties vykdymui specialistai nepasitelkiami
8. PRIEVOLIŲ PAGAL SUTARTĮ ĮVYKDYMO UŽTIKRINIMAS	
8.1. Prievolių pagal Sutartį įvykdymo užtikrinimas	Prievolių pagal Sutartį įvykdymas užtikrinamas: 8.1.1. Netesybomis (delspinigiais, bauda);
8.2 Sutarties įvykdymo užtikrinimo galiojimo terminas	Netaikoma
8.3. Sutarties įvykdymo užtikrinimo pateikimas	Netaikoma
9. ŠALIŲ ATSAKOMYBĖ	
9.1. Pirkėjui taikomos netesybos už mokėjimų pagal Sutartį vėlavimą	Jei Pirkėjas, gavęs tinkamai pateiktą ir užpildytą Sąskaitą, uždelsia atsiskaityti už tinkamai Tiekėjo suteiktas kokybiškas Paslaugas per Sutartyje nurodytą terminą, Tiekėjas nuo kitos nei nustatytas terminas dienos skaičiuoja Pirkėjui 0,05 procento dydžio delspinigius nuo neapmokėtos sumos be PVM už kiekvieną vėlavimo dieną.
9.2. Tiekėjui taikomos netesybos	9.2.1. Jeigu Tiekėjas vėluoja suteikti Paslaugas arba nevykdo kitų sutartinių įsipareigojimų, Pirkėjas nuo kitos nei nustatytas terminas dienos Tiekėjui skaičiuoja 0,05 procento dydžio delspinigius už kiekvieną uždelstą dieną nuo laiku nesuteiktų Paslaugų ar kitų sutartinių įsipareigojimų nevykdymo kainos be PVM. 9.2.2. Tiekėjas privalo sumokėti Pirkėjui netesybas per 30 kalendorinių dienų nuo Pirkėjo pareikalavimo, jeigu netesybų suma nėra išskaitoma iš Tiekėjui mokėtinos sumos. 9.2.3. Už garantinės priežiūros metu, Sutarties priedo Nr. 2 „Techninė specifikacija" 1 priede „Reikalavimai pirkimo objektui" nustatytų klaidų ir trūkumų pašalinimo termino neįgyvendinimą: 9.2.3.1. jeigu tai kritinė klaida ar trūkumas – už kiekvieną kitą darbo dieną taikoma 1 000,00 Eur bauda; 9.2.3.2. jeigu tai nekritinė klaida ar trūkumas – už kiekvieną kitą darbo dieną taikoma 100,00 Eur bauda. 9.2.4. Už garantinės priežiūros metu, Sutarties priedo Nr. 2 „Techninė specifikacija" 1 priede „Reikalavimai pirkimo objektui" nustatytų reakcijos laikų nesilaikymą:

	9.2.4.1. jeigu tai kritinė problema – už kiekvieną kitą valandą taikoma 100,00 Eur bauda; 9.2.4.2. jeigu tai nekritinė problema – už kiekvieną kitą valandą taikoma 10,00 Eur.
9.3. Tiekėjui / Pirkėjui taikoma bauda nutraukus Sutartį dėl esminio Sutarties pažeidimo ar nepagrįstai nutraukus Sutarties vykdymą ne Sutartyje nustatyta tvarka	9.3.1. Nutraukus Sutartį dėl esminio Sutarties pažeidimo, nustatyto Sutarties Specialiosiose sąlygose, mokama 10 procentų dydžio bauda nuo Pradinės Sutarties vertės, nurodytos Specialiųjų sąlygų 5.2 punkte. 9.3.2. Nepagrįstai nutraukus Sutarties vykdymą ne Sutartyje nustatyta tvarka, mokama 10 procentų dydžio bauda nuo Pradinės Sutarties vertės, nurodytos Specialiųjų sąlygų 5.2 punkte.
9.4. Tiekėjui taikoma bauda dėl esamų subtiekėjų ar specialistų pakeitimo / naujų subtiekėjų pasitelkimo nesilaikant Bendrosiose sąlygose nurodytos subtiekėjų ir (ar) specialistų keitimo tvarkos	Tiekėjui, pakeitus 7.1-7.5 p. nurodytą asmenį, nesilaikant Bendrosiose sąlygose nurodytos subtiekėjų ir (ar) specialistų keitimo tvarkos, mokama 1 000,00 Eur bauda už kiekvieną atvejį.
9.5. Tiekėjui taikomos baudos dėl aplinkosauginių ir (arba) socialinių kriterijų nesilaikymo	Netaikoma.
9.6. Tiekėjui / Pirkėjui taikoma bauda dėl konfidencialumo reikalavimų nesilaikymo	Tiekėjui / Pirkėjui nesilaikant Bendrosiose sąlygose nurodytų konfidencialumo reikalavimų, mokama 10 000,00 Eur bauda.
9.7. Tiekėjui taikomos netesybos dėl pirkimo dokumentuose nustatytų kokybinių kriterijų nepasiekimo Sutarties vykdymo metu	Jeigu Tiekėjas Sutarties galiojimo metu neužtikrina atitikties pirkimo dokumentuose nustatytiems kokybiniams kriterijams (ar jo (jų) nepasiekia), už kuriuos Tiekėjui buvo suteikti ekonominio naudingumo balai, mokama žemiau nurodyto dydžio bauda: 1. Už kriterijų „**Tiekėjo siūlomo informacinių sistemų architekto papildoma patirtis**“ – 2,33 proc. nuo nesuteiktų Paslaugų vertės; 2. Už kriterijų **„Tiekėjo siūlomo Backend Programuotojas papildoma patirtis“ –** 2,33 proc. nuo nesuteiktų Paslaugų vertės; 3. Už kriterijų „**Tiekėjo siūlomo Informacinių sistemų analitiko papildoma patirtis“ –** 2,33 proc. nuo nesuteiktų Paslaugų vertės; 4. Už kriterijų **„Tiekėjo siūlomo Projekto vadovo papildoma patirtis“** – 2,33 proc. nuo nesuteiktų Paslaugų vertės;

9.8. Tiekėjui taikomos netesybos dėl Sutarties įvykdymo užtikrinimo nepratęsimo	Netaikoma
9.9. Tiekėjui taikoma bauda dėl Pirkėjo simbolių, pavadinimo ir ženklo reklamoje ar rinkodaroje naudojimo reikalavimų nesilaikymo bei draudimo naudotis Pirkėjo sukurtais intelektiniais veiklos rezultatais nesilaikymo	5 procentai nuo Pradinės Sutarties vertės, nurodytos Specialiųjų sąlygų 5.2 punkte.
9.10. Kitos netesybos ir Sutarties šalių civilinė atsakomybė	**Kitos netesybos:** 9.10.1. Jei specialistas, nurodytas Specialiųjų sąlygų 7 skyriuje, nesant objektyvių priežasčių (tokių kaip specialisto nedarbingumo ir pan.), nedalyvauja iš anksto (ne vėliau, kaip prieš 2 darbo dienas) suplanuotame susitikime, kuriame jo dalyvavimas Pirkėjo vertinimu yra reikalingas, Tiekėjas moka 500,00 (penkių šimtų) Eur baudą. 9.10.2. Jeigu Tiekėjas vėluoja suteikti Paslaugas per Projekto vykdymo plane-grafike nustatytus terminus, Pirkėjas nuo kitos nei nustatytas terminas dienos Tiekėjui skaičiuoja 0,05 procento dydžio delspinigius už kiekvieną uždelstą dieną nuo laiku nesuteiktų Paslaugų ar kitų sutartinių įsipareigojimų nevykdymo kainos be PVM.
10. ESMINĖS SUTARTIES SĄLYGOS	
10.1. Esminės Sutarties sąlygos	Specialiųjų sąlygų 12.2. p. nurodyti įsipareigojimai kurių nesilaikymas bus laikomas esminiu pažeidimu.
11. SUTARTIES GALIOJIMAS IR KEITIMAS	
11.1. Sutarties sudarymas ir įsigaliojimas	Ši Sutartis laikoma sudaryta ir įsigalioja nuo Sutarties pasirašymo dienos (antrosios Šalies pasirašymo dieną). Sutartis galioja iki visiško prievolių įvykdymo (kol bus išnaudota Pradinės Sutarties vertė, bet jos terminas negali būti ilgesnis kaip **86 mėnesiai** (įskaitant galimus Paslaugų suteikimo ir teikimo termino pratęsimus bei apmokėjimo už Paslaugas terminus).
11.2. Sutarties galiojimo termino pratęsimas	Netaikoma
12. SUTARTIES NUTRAUKIMAS	
12.1. Sutarties nutraukimo pagrindai	Sutartis gali būti nutraukiama rašytiniu Šalių susitarimu arba vienašališkai, Bendrosiose sąlygose nustatyta tvarka.
12.2. Esminiai Sutarties pažeidimai	12.2.1. jeigu Tiekėjas nevykdo prisiimtų įsipareigojimų už Sutartyje nustatytą Sutarties kainą / įkainius; 12.2.2. jeigu Tiekėjas nepateikia Sutarties įvykdymo užtikrinimo pratęsimo ilgiau kaip 30 dienų nuo galiojančio Sutarties įvykdymo užtikrinimo termino pabaigos Bendrosiose sąlygose nustatyta tvarka (išskyrus pirminį Sutarties įvykdymo užtikrinimą)

	(nuostata taikoma, kai Sutarties įvykdymas užtikrinamas ir kitais, nei Sutarties 8.1.1. p. nurodytais būdais); 12.2.3. jeigu paaiškėja, kad Tiekėjas nevykdo įsipareigojimų, kurie pasiūlymų vertinimo metu pirkimo dokumentuose buvo nustatyti kaip pasiūlymų vertinimo kriterijai ir už kuriuos Tiekėjui buvo skiriamos reikšmės, kai pasiūlymas vertintas pagal kainos / sąnaudų ir kokybės santykį ir Tiekėjas per 30 kalendorinių dienų neištaiso pažeidimų **(nuostata taikoma, kai pasiūlymas vertintas pagal kainos / sąnaudų ir kokybės santykį)**; 12.2.4. jeigu Tiekėjas nesilaiko Sutartyje nustatytų Paslaugų teikimo terminų 2 (du) kartus iš eilės arba vėluoja suteikti Paslaugas daugiau nei 20 darbo dienų nuo Sutartyje nustatyto Paslaugų suteikimo termino; 12.2.5. jeigu Tiekėjas pažeidžia Paslaugų suteikimo terminus ir priskaičiuotų netesybų už vėlavimą suma viršija 20 proc. Pradinės sutarties vertės; 12.2.6. Tiekėjas pažeidžia Paslaugų suteikimo terminus ir dėl Paslaugų suteikimo vėlavimo Paslaugos tampa nebereikalingos; 12.2.7. Tiekėjas daugiau kaip 2 kartus suteikia Paslaugas, kurios neatitinka Sutartyje ir (ar) įstatymuose nustatytų reikalavimų Paslaugoms; 12.2.8. Tiekėjo kvalifikacija tapo nebeatitinkančia pirkimo dokumentuose nustatytų Sutarties tinkamam vykdymui būtinų reikalavimų ir šie neatitikimai nebuvo ištaisyti per 10 darbo dienų nuo kvalifikacijos tapimo neatitinkančia dienos **(nuostata taikoma, kai pirkimo dokumentuose buvo nustatyti reikalavimai tiekėjų kvalifikacijai)**; 12.2.9. Tiekėjas pažeidžia šios Sutarties nuostatas, reglamentuojančias konkurenciją, intelektinės nuosavybės ar konfidencialios informacijos valdymą; 12.2.10. Tiekėjas pažeidžia Bendrųjų sąlygų nuostatas dėl Sutarties vykdymui pasitelkiamų naujų subtiekėjų ir (ar) specialistų / esamų subtiekėjų ir (ar) specialistų keitimo; 12.2.11. Tiekėjas ir (ar) jungtinės veiklos partneris (jei taikoma), ir (ar) subtiekėjas (jei taikoma) Paslaugų, kurioms Sutartyje nustatyti aplinkos apsaugos vadybos sistemos reikalavimai, teikimo metu, neturi galiojančio aplinkos apsaugos vadybos sistemos sertifikato, ir (ar) nepateikia sertifikato pratęsimo (neįsigyja naujo) **(nuostata taikoma, kai pirkimo dokumentuose buvo nustatyti aplinkos apsaugos vadybos sistemos reikalavimai)**; 12.2.12. Tiekėjas 2 (du) kartus pažeidžia esminę Sutarties sąlygą; 12.2.13. paaiškėjo, kad su Tiekėju neturėjo būti sudaryta Sutartis dėl to, kad Europos Sąjungos Teisingumo Teismas procese pagal Sutarties dėl Europos Sąjungos veikimo 258 straipsnį pripažino, kad nebuvo įvykdyti įsipareigojimai pagal Europos Sąjungos steigiamąsias sutartis ir Direktyvą 2014/24/ES;

	12.2.14. Lietuvos Respublikos Vyriausybė Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo nustatyta tvarka priima sprendimą, patvirtinantį, kad Sutartis (jo pakeitimas) laikoma keliančia riziką ar neatitinka nacionalinio saugumo interesų; 12.2.15. Sutartis buvo pakeista pažeidžiant Viešųjų pirkimų įstatymo 89 straipsnį; 12.2.16. paaiškėjo, kad Tiekėjas, su kuriuo sudaryta Sutartis, turėjo būti pašalintas iš Pirkimo procedūros pagal Viešųjų pirkimų įstatymo 46 straipsnio 1 dalį; 12.2.17. paaiškėjo Viešųjų pirkimų įstatymo 37 straipsnio 9 dalyje, 45 straipsnio 2^1 dalyje ir (ar) 47 straipsnio 9 dalyje nurodytos aplinkybės.
13. APLINKOS APSAUGOS IR SOCIALINIAI KRITERIJAI	
13.1. Su perkamomis paslaugomis susiję aplinkos apsaugos kriterijai	Netaikoma
13.2. Su perkamomis Paslaugomis susiję socialiniai kriterijai	Netaikoma
14. BENDRŲJŲ SĄLYGŲ PAKEITIMAI IR PAPILDYMAI	
14.1.	Šalys susitaria pakeisti Sutarties Bendrųjų sąlygų **1.3.1 punktą** ir išdėstyti jį nauja redakcija: „1.3.1. Sutartį sudarantys dokumentai turi būti suprantami kaip papildantys vienas kitą. Bet kokio Sutarties dokumentų sąlygų neatitikimo ar neaiškumo atveju, toks neatitikimas ar neaiškumas pašalinamas dokumentus aiškinant tokia eilės tvarka: 1.3.1.1. Specialiosios sąlygos 1.3.1.2. Techninė specifikacija; 1.3.1.3. Bendrosios sąlygos; 1.3.1.4. Pirkimo dokumentai (išskyrus techninę specifikaciją); 1.3.1.5. Pasiūlymas; 1.3.1.6. Kiti Specialiosiose sąlygose išvardinti priedai.“
14.2.	Sutarties Bendrosiose sąlygose nurodytos alternatyvios nuostatos (su prierašu „jei taikoma“ ir pan.) taikomos tik tokiu atveju, jeigu jos konkrečiai aprašomos Sutarties Specialiosiose sąlygose.
14.3.	Šalys susitaria papildyti Sutarties Bendrąsias sąlygas nurodytu punktu, tačiau kitų punktų numeracijos nekeisti: „17.7. Tiekėjui rekomenduojama vykdant Sutartį laikytis Viešųjų pirkimų tarnybos parengto Tiekėjų etikos kodekso nuostatų[1]. Tiekėjas įsipareigoja užtikrinti Tiekėjų etikos kodekso 35-37 p. nuostatų laikymąsi visą Sutarties galiojimo laikotarpį.“
14.4.	Tuo atveju jei bus gautas Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos siūlymas, Šalys susitaria papildyti Sutarties Bendrąsias sąlygas nurodytu punktu, tačiau kitų punktų numeracijos nekeisti:

[1] Viešųjų pirkimų tarnybos parengtas Tiekėjų etikos kodeksas, https://vpt.lrv.lt/media/viesa/saugykla/2024/1/w2fscibRf-4.pdf

	„16.5. Tiekėjas įsipareigoja neteikti jokios informacijos Rusijos Federacijos, Baltarusijos Respublikos, Kinijos Liaudies Respublikos subjektams (ar jiems atstovaujantiems asmenims) ir užtikrinti, kad šių valstybių subjektai nebūtų pasitelkiami dalyvauti šioje Sutartyje jokiomis formomis." Arba nurodomas kitas Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos siūlymas (jei toks bus gautas).
14.5.	Šalys susitaria pakeisti Sutarties Bendrųjų sąlygų 17.2. punktą ir išdėstyti jį nauja redakcija: „17.2. Netesybų sumokėjimas ir (ar) Sutarties įvykdymo užtikrinimo gavimas nepanaikina Šalies teisės reikalauti, kad kita Šalis kompensuotų jos patirtus tiesioginius nuostolius ar žalą bei papildomas išlaidas. Šioje Sutartyje nustatytos netesybos yra laikomos minimaliais, neįrodinėtinais Šalių nuostoliais. Kiekviena iš Šalių turi teisę gauti iš kitos Šalies nuostolių, atsiradusių dėl kitos Šalies netinkamo įsipareigojimų pagal Sutartį vykdymo ar nevykdymo, neviršijant Pradinės sutarties vertės, jei teisės aktai nenumato, kad privalo būti kompensuota didesnė suma. Šiame punkte numatytas atsakomybės ribojimas netaikomas, jei žala atsirado dėl konfidencialumo įsipareigojimų, asmens duomenų apsaugą reglamentuojančių teisės aktų ar intelektinės nuosavybės teisių pažeidimo."
14.6.	Šalys susitaria papildyti Sutarties Bendrąsias sąlygas nurodytu punktu, tačiau kitų punktų numeracijos nekeisti: „3.2.15 Užsakovas netikrina specialistų atitikties Pirkimo dokumentuose nustatytiems kvalifikacijos reikalavimams, jeigu pasitelkiami papildomi specialistai, nurodyti Sutarties Specialiųjų sąlygų 7.5 punkte".
15. SUTARTIES PRIEDAI	
15.1. Priedas Nr. 1	Bendrosios sąlygos
15.2. Priedas Nr. 2	Techninė specifikacija
15.3. Priedas Nr. 3	Pasiūlymas
15.4. Priedas Nr. 4	Paslaugų perdavimo-priėmimo akto forma
15.7. Priedas Nr. 5	Defektų aktas
15.5. Priedas Nr. 6	Asmens duomenų tvarkymo susitarimas
15.6. Priedas Nr. 7	Susitarimas dėl taikomų organizacinių ir techninių kibernetinio saugumo reikalavimų
16. ŠALIŲ ATSTOVŲ PARAŠAI	
PIRKĖJAS	**TIEKĖJAS**
Generalinis direktorius	Generalinis direktorius
(parašas)	**(parašas)**

Paslaugų viešojo pirkimo–pardavimo sutarties specialiosios dalies Nr. ST-
Priedas Nr. 4

(perdavimo–priėmimo akto forma)

PASLAUGŲ perdavimo–priėmimo aktas

Nr.

_____

(sudarymo vieta)

Šį aktą pasirašę atsakingi asmenys pažymi, kad vadovaudamiesi pasirašytos *[Įrašyti sutarties pavadinimą Nr. XX-XXX]* (toliau – Sutartis), Tiekėjas perduoda, o Pirkėjas priima šioje lentelėje nurodytas Paslaugas:

Eil. Nr.	Paslaugų pavadinimas	Veiklos kodas*	Mato vnt.	Kiekis	Vieneto kaina, Eur be PVM	Suma, EUR be PVM
1.		[Pasirinkite]				
2.		[Pasirinkite]				
3.		[Pasirinkite]				
					Iš viso:	
					PVM (nurodyti) %:	
					Bendra suma:	

** Veiklos kodas derinamas su Pirkėju.*

Tiekėjas suteikė visas Paslaugas ir pateikė visus reikiamus dokumentus pagal Sutartį
Pasirinkti

PASLAUGAS PRIĖMĖ:
Valstybės įmonė Registrų centras

_____

(atsakingo asmens pareigų pavadinimas)
(vardas ir pavardė)

PASLAUGAS PERDAVĖ:
(Tiekėjo pavadinimas):

_____

(atsakingo asmens pareigų pavadinimas)
(vardas ir pavardė)

Paslaugų viešojo pirkimo–pardavimo sutarties specialiosios dalies Nr. ST-
Priedas Nr. 5

(Defektų akto forma)

DEFEKTŲ AKTAS
Nr.

_____
(sudarymo vieta)

Pažymime, kad vadovaudamiesi pasirašytos *[Įrašyti sutarties pavadinimą Nr. XX-XXX]* (toliau – Sutartis), Pirkėjas nustatė šioje lentelėje nurodytus Paslaugų ir / ar su Paslaugomis susijusių prekių ir / ar Tiekėjo pateiktų dokumentų trūkumus:

Eil. Nr.	Paslaugų / su Paslaugomis susijusių prekių / dokumentų trūkumų aprašymas	Trūkumų pašalinimo tvarka	Trūkumų pašalinimo terminas
1.			
2.			
3.			
...			

_____	_____	_____
(Už Sutarties vykdymą atsakingo asmens pareigų pavadinimas)	(Parašas)	(vardas ir pavardė)

GENERAL CONDITIONS OF THE CONTRACT FOR THE PUBLIC PROCUREMENT-SALE OF THE SERVICES

1. BASIC CONCEPTS, DEFINITONS AND INTERPRETATION OF THE CONTRACT

1.1. Concepts and definitions

1.1.1. The capitalised terms used in the Contract shall have the meaning as provided below:
1.1.1.1. **General Conditions** shall mean the part of the Contract, which is referred to as 'General Conditions of the Contract for the Public Procurement-Sale of the Services';
1.1.1.2. **Buyer** shall mean a person named as the Buyer in the Special Conditions who procures the Services specified in the Special Conditions and Annexes to the Contract;
1.1.1.3. **Initial Contract Value** shall mean the value indicated in the Special Conditions excluding Value-Added Tax (hereinafter referred to as the VAT);
1.1.1.4. **Services** shall mean the services specified in the Special Conditions and the Annexes to the Contract. The term 'Services' used in the Contract shall include all activities related to the provision of the Services, including, but not limited to, the provision of the Services, transfer of their results, elimination of defects, supply of products and submission of the documents related to the Services (instructions, certificates, etc.) if this is provided for in the Contract, or is necessary for the creation and transfer of the Service results to the Buyer;
1.1.1.5. **Statement of Transfer and Acceptance of the Services** shall mean the document by which the Provider transfers and the Buyer accepts the Services and/or the Service results, and by which the Parties certify that the provided Services meet the specified requirements. If the Contract provides for the phased provision of the Services or their provision in periods, the Statement of Transfer and Acceptance of the Services may be concluded for each phase or period separately;
1.1.1.6. **Service Defects** shall mean non-compliance of the quality of the provision or the Service results identified by the Buyer or/and third parties at any time during the Contract or during the warranty period of the Services with the requirements of the Contract or/and laws and other legal acts, hidden defects, disruptions in the operation, etc., which would prevent the use of the Service results for the purpose the Buyer intended to use them (the Services), or which would reduce the benefits and efficiency of the Services in such a way that the Buyer, knowing of such defects, would not have procured the Services at all, or would not have paid such a price for the Services;
1.1.1.7. **Invoice** shall mean the invoice, VAT invoice or other payment document issued by the Provider and submitted to the Buyer for payment for the Services duly delivered by the Provider and accepted by the Buyer. If the Contract provides for the phased provision of the Services or their provision in periods, the Invoice may be issued for each phase or period separately;
1.1.1.8. **Special Conditions** shall mean the part of the Contract, which is referred to as 'Special Conditions of the Contract for the Public Procurement-Sale of the Services' and which contains terms and conditions (such as the Initial Contract Value, time limits for the provision of the Services, etc.) and other specific data (such as Parties, Services, etc.) describing procurement of a Procurement object, listed annexes, as well as specified changes and supplements to the General Conditions (if any);
1.1.1.9. **Arrangement** shall mean a document concluded by the Parties in the course of amending the terms and conditions of the Contract to the extent permitted by the Law on Public Procurement;
1.1.1.10. **Contract Price** shall mean the amount payable to the Provider under the Contract, including

any mandatory fees, charges and costs;

1.1.1.11. **Conditions of the Contract** shall mean General Conditions and Special Conditions together;

1.1.1.12. **Contract** shall mean a Contract for the Public Procurement-Sale of the Services consisting of the Conditions of the Contract, annexes and arrangements listed in the Special Conditions;

1.1.1.13. **Party** shall mean the Buyer or the Provider, each individually, depending on the context;

1.1.1.14. **Parties** shall mean the Buyer and the Provider jointly;

1.1.1.15. **Provider** shall mean a person named as a provider in the Special Conditions who provides the Services referred to in the Special Conditions;

1.1.1.16. **Order** shall mean a written order of the Buyer for the provision of the Services sent to the Provider (as a text message, e-mail, via the information system specified by the Buyer, etc.). The Order shall be sent by the means and to the contacts specified in the Special Conditions and shall be considered properly sent and received in accordance with the procedure laid down in the Special Conditions;

1.1.1.17. **Law on Public Procurement** shall mean the Law of the Republic of Lithuania on Public Procurement.

1.1.1.18. The meanings of other capitalised terms in the Contract shall be specified in the text of the Agreement.

1.1.2. Concepts not defined in the Contract shall be understood and interpreted as defined by the Law on Public Procurement and other laws and legal acts in force at the time of conclusion and performance of the Contract.

1.1.3. Other concepts and definitions used in the Contract shall have a general meaning or a special meaning closest to the nature of the Contract unless otherwise specified and explained in the Contract.

1.2. Interpretation of the Contract

1.2.1.The Contract shall be concluded and interpreted in accordance with legal acts of the Republic of Lithuania.

1.2.2.If the General Conditions and/or Special Conditions contradict the requirements of the Law on Public Procurement and other legal acts, the provisions of the Law on Public Procurement and other legal acts shall apply.

1.2.3.A day in the Contract shall mean a calendar day.

1.2.4.A working day in the Contract shall mean any day, except Saturday, Sunday and holidays in Lithuania as indicated in the Labour Code of the Republic of Lithuania.

1.2.5.Time limits under the Contract shall be estimated in years, months, weeks, weekdays, calendar days, hours and minutes.

1.2.6.Qualification, reliance on the capacities of other economic operators, scope of the Services, review shall be understood as laid down in the Law on Public Procurement and the secondary legislation.

1.2.7.Where the requirement of a Statement on the Transfer and Acceptance of the Services as a separate document is not mandatory, the Parties shall agree thereon and expressly refer thereto in the Special Conditions: Invoice shall be deemed to be the Statement on the Transfer and Acceptance of the Services. In cases where an Invoice is issued and the Statement on the Transfer and Acceptance of the Services is not signed, provisions of the Contract on the issue of the Statement on the Transfer and Acceptance of the Services shall also apply to the issue of Invoice.

1.2.8.To inform, notify, warn or respond shall mean to provide information, notification, warning or

response in accordance with the procedure laid down in the General and/or Special Conditions.
1.2.9.To approve shall mean to submit a written confirmation or to sign the document without reservation or subject to reservation unless the person, when signing the document, states that they refuse to approve it.
1.2.10. Unless otherwise stated in the Contract, words used in singular form shall also mean plural form and vice versa; words of one family shall include the corresponding words of another family; the word 'person' shall mean both natural persons and legal entities.
1.2.11. If the meaning expressed in numbers and words differs in the Contract, the meaning given in words shall be adhered to.
1.2.12. If references to legal acts are provided, the updated versions of the legal acts must be applied unless otherwise specified.

1.3.Primacy of documents

1.3.1.The documents constituting the Contract shall be understood as complementing each other. In the event of any inconsistency or ambiguity in the conditions of the Contract documents, such inconsistency or ambiguity shall be eliminated by interpreting the documents in the following order of priority:
1.3.1.1. Technical Specification;
1.3.1.2. Special Conditions;
1.3.1.3. General Conditions;
1.3.1.4. Procurement documents (except for Technical Specification);
1.3.1.5. Tender bid;
1.3.1.6. Other annexes listed in Special Conditions.
1.3.2. In the event the Conditions of the Contract are changed by the Arrangement of the Parties, the newly agreed Conditions of the Contract shall prevail over the modified ones.
1.3.3.If the Parties conclude an Arrangement on the addition of a new condition to the Conditions of the Contract or to the Annex, in the event of inconsistency or ambiguity, such a condition shall have primacy over the other Conditions of the Contract or other conditions of that Annex as appropriate.
1.3.4.If the Parties agree on a new Annex, the Parties shall agree on the ranking of the new Annex in the list of Annexes and its significance for the interpretation of the Contract. If a new Annex is inserted into the list of Annexes, it shall be assigned a sequence number with the upper index, considering the order of priority and importance of Annexes (e.g. Annex No 4^{1}).

2. SUBJECT-MATTER OF THE CONTRACT

2.1. The Provider undertakes to provide the Services, which comply with the requirements of the Contract, under the conditions and in accordance with the procedure laid down in the Contract to the Buyer, and the Buyer undertakes to accept the Services, which comply with the conditions of the Contract and have been properly provided, and to pay the Provider the price specified in the Contract under the conditions and procedure laid down therein.
2.2. When performing the Contract, the Parties undertake to comply with all the requirements of laws and other legal acts applicable to the performance of the Contract. A Party shall have the right to require the other Party to comply with all the requirements of laws and legal acts applicable to the performance

of the Contract. None of the conditions of the Contract shall be and may not be construed as a waiver by the Buyer of any other rights and guarantees established in laws or other legal acts and not covered in the Contract regarding the improper provision or quality of the Services, or as a waiver by the Provider of other rights and guarantees established in laws or other legal acts and not covered in the Contract regarding the receipt of payment for the Services.

2.3. The Provider shall ensure that the Services meet the requirements of the Technical Specification and conditions of the Provider's tender bid, are of high quality, delivered in a timely and appropriate manner in accordance with the terms and conditions of the Contract and in such a way that it is the most responsive to the interests of the Buyer, in accordance with the best generally accepted professional, technical standards and practices, using all the necessary skills and knowledge.

3. PROVIDER AND OTHER PERSONS INVOLVED FOR THE PERFORMANCE OF THE CONTRACT

3.1. Qualifications and other obligations assumed by the Provider in the tender bid

3.1.1. The Provider shall be responsible for ensuring that they are competent, reliable and capable (including the capacity of the economic operators whose capacity the Provider relies on) of fulfilling the requirements of the Contract throughout the term thereof:

3.1.1.1. Have the right to engage in the activities necessary for the performance of the Contract; Upon the Buyer's request, the Provider shall provide documents proving that the Contract is performed only by persons entitled to do so;

3.1.1.2. Meet the mandatory requirements laid down in the Procurement documents for the qualification of tenderers and do not have grounds for exclusion laid down in the Procurement documents;

3.1.1.3. Comply with the obligations set out in the tender bid, including, but not limited to, values and parameters of the qualitative, environment and/or social criteria (hereinafter referred to as the **Qualitative Criteria**) set out in the Procurement documents. The procedure for checking compliance with the obligations referred to in this point shall be laid down in the Specific Conditions;

3.1.1.4. Ensure the imposition of the established quality management system and/or environmental management system standards, where required by the Procurement documents, and have the supporting documents;

3.1.1.5. Comply with the interests of national security and not to be registered (permanently residing or having citizenship) in the countries or territories deemed to be unreliable if such requirements were established in the Procurement documents.

3.1.2. In the event the Provider is a group of providers operating under the joint venture agreement, they shall be jointly and severally liable to the Buyer for the performance of the Contract. If the Provider relies on the capacities of economic operators to meet the requirements of financial and economic capacity, the Provider shall be jointly and severally liable with such economic operators for the performance of the Contract (if required in the Procurement documents).

3.1.3. The Provider shall also be responsible for ensuring that they, the sub-providers and specialists directly engaged in the Contract comply with the professional qualifications and other requirements laid down by laws and other legal acts and/or Procurement documents and have the right to engage in the activities for which they are engaged.

3.2. The use and replacement of sub-providers and specialists

3.2.1.The Provider undertakes to ensure that the Contract will be performed by the sub-providers and/or specialists who meet the requirements set out in the Procurement documents. The actions of these persons in the performance of the Contract shall have the same consequences and liability to the Provider as their own actions. The Provider shall be responsible for the acts or omissions of its sub-providers and specialists.
3.2.2.Sub-providers and/or specialists involved for the performance of the Contract (if involved) shall be specified in the Special Conditions.
3.2.3.The Provider may change and/or involve the sub-providers and/or specialists specified in the Contract in cases and following the procedure specified in this Section of the Contract.
3.2.4. A new sub-provider or a specialist may begin to fulfil their obligations assigned by the Provider under the Contract no earlier than the date of signature of the Arrangement.
3.2.5. If the Provider involves a new sub-provider or replaces the existing sub-provider or the specialist without a written consent of the Buyer, or contractual obligations are performed by sub-providers or specialists who do not meet the qualification requirements established in the Procurement documents, quality management system and/or environmental management system standards, the requirements on the absence of grounds for exclusion, compliance with national security interests and requirements not to be registered (permanently residing or having citizenship) in the countries or territories deemed to be unreliable (if applicable) as well as the conditions specified in the tender bid to justify the qualitative criteria set out in the Procurement documents (if applicable), the Provider shall be subject to a penalty charge established in the Special Conditions.
3.2.6. The Provider shall have the right to involve new sub-providers for the performance of the Contract who were not specified in Special Conditions and whose capacity has not been used to justify the qualification requirements provided for in the Procurement documents.
3.2.7. Upon conclusion of the Contract but not later than the commencement of performance of the Contract, the Provider undertakes to inform the Buyer of the names, code of legal entity, contact details and representatives of the sub-providers known at that time whose capacity has not been used by the Provider to justify the qualification requirements provided for in the Procurement documents.
3.2.8. The Provider may, at any time during the performance of the Contract, change sub-providers whose capacity has not been used by the Provider to justify the qualification requirements provided for in the Procurement documents at its own discretion.
3.2.9. The Provider shall inform the Buyer of the involvement and/or change of a new sub-provider whose capacity the Provider has not relied on to justify the qualification requirements provided for in the Procurement documents at any time during the performance of the Contract and not later than 5 (five) working days before the involvement and/or change thereof. The Buyer (if applicable in the Procurement documents) must check the absence of grounds for exclusion of the sub-provider and the sub-provider's compliance with national security interests and requirements not to be registered (permanently residing or having citizenship) in the countries or territories deemed to be unreliable. If the situation of the sub-provider does not meet at least one of the said requirements, the Buyer shall require the replacement of the sub-provider by someone who meets the requirements. The Buyer shall inform the Provider in writing within 5 (five) working days of the consent to use and/or replace a new sub-provider whose capacity the Provider has not relied on in support of the qualification requirements

provided for in the Procurement documents. When the Buyer has agreed, the Parties shall sign an Arrangement, which shall be considered an integral part of the Contract.

3.2.10. The sub-providers whose capacity the Provider has relied on to meet the qualification requirements established in the Procurement documents may be changed only in the following cases:

3.2.10.1. Where a sub-provider is subject to insolvency proceedings or out-of-court bankruptcy proceedings, they become insolvent or there is a probability of insolvency, they suspend economic activity or when similar situations arise in accordance with the procedure laid down in laws and other legal acts;

3.2.10.2. Where a sub-provider is no longer able to fulfil all or part of the obligations provided for in the Contract for objective reasons (e.g. if the sub-provider refuses to participate in the performance of the Contract, if legal relationship with the Provider is terminated, etc.).

3.2.10.3. The Provider or the sub-provider must replace the sub-provider if it appears that they do not meet the requirements established in the Procurement documents.

3.2.11. The specialists of the Provider (or sub-providers) who are going to perform the Contract may be replaced in the following cases:

3.2.11.1. At the initiative of the Provider for objective reasons (such as holidays, illness, termination of employment relations, etc.) after provision of the data on a new specialist who is going to be appointed and their qualifications as well as documents proving compliance with other requirements established in the Procurement documents;

3.2.11.2. At the initiative of the Buyer if the Buyer has reasonable suspicions that the specialist appointed by the Provider for the performance of the Contract is not competent to perform the prescribed duties.

3.2.11.3. The Provider or the sub-provider must replace the specialist if it appears that they do not meet the requirements established in the Procurement documents.

3.2.12. A new specialist and/or sub-provider must meet the requirements for the specialist and/or sub-provider provided for in the Procurement documents at the time of the submission of the Provider's request to replace the specialist and (or) sub-provider.

3.2.13. The Provider shall provide the Buyer with the following documents not later than 5 (five) working days before the planned replacement of the sub-provider whose capacity the Provider has relied on to meet the qualification requirements established in the Procurement documents, and/or the specialist:

3.2.13.1. A reasoned written request to change a sub-provider and/or a specialist, explaining the reasons of replacement. The Buyer shall reserve the right to request evidence to support the reasons of replacement;

3.2.13.2. Documents proving the qualification of a new sub-provider and/or specialist, compliance with the required quality management system and/or environmental management system standards (if applicable), the absence of grounds for exclusion and compliance with national security interests and requirements not to be registered (permanently residing or having citizenship) in the countries or territories deemed to be unreliable (if applicable) in accordance with the requirements of the Contract.

3.2.14. Upon receipt of the Provider's request along with other documents specified in the Contract, the Buyer shall evaluate the possibilities of replacement within 5 (five) working days and inform the Provider in writing of the consent to replace the sub-provider whose capacity the Provider relied on to meet the qualification requirements provided for in the Procurement documents and/or the specialist. When the Buyer has agreed, the Parties shall sign an Arrangement, which shall be considered an integral part of the Contract.

3.3. Replacement of joint venture partners

3.3.1. The Provider, performing the Contract as a group of providers within the framework of joint activity agreement, shall have the right to eliminate a joint venture partner (hereinafter referred to as the Partner) if due to objective and reasonable circumstances the Partner is no longer able to perform the Contract, including, but not limited to cases where the Partner does not comply with the provisions of the Law on Public Procurement or other legal acts, poses a threat to national security; the Partner has been imposed international sanctions within the meaning of the Law on International Sanctions of the Republic of Lithuania (hereinafter referred to as the Law on Sanctions); the Partner is in difficult financial situation resulting in the non-performance of the Contract and/or refusal to perform it; or other objective reasons for the withdrawal of the Partner from the joint venture agreement has arisen.
3.3.2. The Provider, performing the Contract as a group of providers within the framework of joint activity agreement, shall have the right to replace the Partner if, due to reorganisation, restructuring or bankruptcy proceedings, the rights and obligations of the original Partner are wholly or partly taken over by the other Partner. Such replacement of the Partner shall not lead to other substantial changes to the Contract and shall not be aimed at avoiding the application of the Law on Public Procurement and other legal acts.
3.3.3. The Provider shall submit to the Buyer the following documents not later than 10 (ten) working days before the intended replacement or elimination of the Partner:
3.3.3.1. A reasoned written request to change the composition of the Provider and evidence justifying at least one circumstance for elimination of the Partner or its replacement specified in the Contract;
3.3.3.2. A draft of the new joint venture agreement or the draft amendment to the existing joint venture agreement stating that, if the Partner withdraws, the obligations of the withdrawing Partner are fully taken over by the remaining Partner and/or a newly involved Partner;
3.3.3.3. Documents confirming the qualification of the remaining Partner or a newly involved Partner and, if applicable, documents proving the requirements of quality management and/or environmental management system standards. In all cases, the qualification of the remaining Partner or a new Partner must not be lower than that of the withdrawing Partner (meeting the qualification requirements established in the Procurement documents, which were met by the withdrawing Partner and meeting the qualification of specialists specified in the tender bid of the withdrawing Partner and other conditions to support the qualitative criteria established in the Procurement documents (if applicable). Where a new Partner is involved, documents shall also be provided, in accordance with the requirements specified in the Procurement documents, justifying the absence of grounds for exclusion of the Partner involved and compliance with national security interests and requirements not to be registered (permanently residing or having citizenship) in the countries or territories deemed to be unreliable (if applicable).
3.3.4. Upon receipt of the Provider’s request with other documents specified in the Contract, the Buyer shall evaluate the possibilities of replacement within 10 (ten) working days and inform the Provider in writing about the consent to eliminate or replace the Partner or about the rejection of the request. When the Buyer has agreed, the Parties shall sign an Arrangement, which shall be considered an integral part of the Contract. Before signing the Arrangement, the Buyer shall be provided with a copy or transcript of the new joint venture agreement or amendment of the existing joint venture agreement.

3.4. Agreements on direct payment to sub-providers

3.4.1.If the sub-providers so request, the Buyer shall pay them directly. The Buyer shall provide for the direct payment option to the sub-providers specified in the Contract under the following conditions and procedure:
3.4.1.1. Upon conclusion of the Contract and not later than the commencement of performance of the Contract, the Provider undertakes to inform the Buyer in writing of the names, contact details and representatives of the sub-providers known at that time. The Buyer shall also require the Provider to inform about the changes in the said information during the entire performance of the Contract;
3.4.1.2. The Buyer shall inform sub-providers in writing about the direct payment option not later than within 3 (three) working days from the date of receipt of the information specified in point 3.4.1.1 of the General Conditions;
3.4.1.3. To take advantage of such an opportunity, the sub-provider shall submit a written request to the Buyer. Where the sub-provider expresses its wish to make use of the direct payment option, a tripartite agreement shall be concluded between the Buyer, the Provider and that sub-provider, which describes the procedure for direct payment to the sub-provider, considering the requirements set out in the Contract and the sub-provision agreement;
3.4.1.4. The direct payment option to sub-providers shall not relieve the Provider of the responsibility for the performance of the Contract.

4. COOPERATION BETWEEN THE PARTIES

4.1. Duty of cooperation between the Parties

4.1.1.In the performance of the Contract, the Parties shall cooperate to the fullest extent possible and exchange information promptly, as well as submit written notifications of the occurrence or existence of any event, condition or circumstance, which may affect the performance of the Contract or cause its breach, to each other without delay.
4.1.2.The Parties undertake to ensure that they provide each other with documents and/or other information necessary for the proper performance of their obligations under the Contract.
4.1.3.If a Party encounters an obstacle to the implementation of the Contract, it shall immediately but not later than within 5 (five) working days warn the other Party of such obstacles and take all reasonable measures within its power to remove those obstacles.

4.2. Contact persons

4.2.1.Each Party must appoint a contact person responsible for the performance of the Contract (e.g., acceptance of the Service result, delivery and receipt of Orders, etc.) at the time of conclusion of the Contract and specify their contact details in the Special Conditions.
4.2.2.In the event a Party wishes to revoke the designated contact person and appoint another person or wishes to appoint another person to perform the contact person’s functions during the period of temporary inability of the contact person to perform its functions, the Party must inform the other Party thereof in advance and provide the other Party with the contact details of such person: name, surname, e-mail and telephone number.

4.2.3.In the event it becomes apparent that the contact person of a Party is temporarily unable to perform its duties (due to illness, injury or other unforeseen reasons), the Party must immediately but not later than the next working day appoint another contact person to perform the functions of the contact person on a temporary basis and notify the other Party. In the event of replacement of the persons performing the functions of contact persons, the Arrangement shall not be concluded in accordance with point 20.5 of the General Conditions.

5. DOCUMENTS PROVIDED DURING THE PERFORMANCE OF THE CONTRACT

5.1. If the Provider has to prepare and/or provide the Buyer with instructions for the use of the Service results, they must be clear and detailed so that the Buyer can properly use the Service results following the said instructions.
5.2. In the event training and/or testing is required under the Contract, the Provider shall send instructions for use prior to such training and/or testing to the Buyer, and it shall revise and supplement the instructions for use after training and/or testing, having considered the progress and results of training and/or testing.
5.3. If the documents necessary for the use of the Service results require translation, the Provider shall bear the costs thereof. If the Provider translates the documents necessary for the use of the Service results independently, it shall be responsible for the accuracy of translation of these documents.

6. COMPLETION OF PROVISION OF THE SERVICES AND ACCEPTANCE OF THE SERVICE RESULTS

6.1. Completion of provision of the Services

6.1.1.Provision of the Services shall be deemed to have been completed when all the following conditions are met:
6.1.1.1. The Provider has provided all Services in accordance with the requirements of the Contract as well as laws and other legal acts;
6.1.1.2. The Provider has transferred to the Buyer all necessary documentation, including instructions for use, certificates and guarantees (if required);
6.1.1.3. The Provider has trained the Buyer's staff on how to use the Service result (if required);
6.1.1.4. The Statement on the Transfer and Acceptance of the Services or Statements on the Transfer and Acceptance of the Services have been signed in case the Services are to be provided in phases or in periods, or any other document provided for in the Contract has been signed and the Services are deemed to have been accepted from signature of the said document;
6.1.1.5. The Provider has fulfilled other conditions provided for in the laws and other legal acts, in the Contract and the tender bid, which must be fulfilled to consider the provision of the Services to be completed and has provided the Buyer with documents proving this.

6.2. Transfer and acceptance of the Services, which are provided once, periodically or upon the Buyer's Order

6.2.1.The Provider must provide the Services and transfer the Service result to the Buyer (if applicable),

and the Buyer must accept the good quality Services that meet the requirements of the Contract and laws as well as other legal acts. The Services must be provided in the manner and within the time limits specified in the Special Conditions.

6.2.2.The Service result shall be transferred to the Parties by signing the Statement on the Transfer and Acceptance of the Services, which is executed in 2 (two) copies with the same legal effect (except where the Statement on the Transfer and Acceptance of the Services is signed with a secure electronic signature, one for each Party). Where the requirement of a Statement on the Transfer and Acceptance of the Services as a separate document is not mandatory, the Parties shall agree thereon and expressly refer thereto in the Special Conditions: Invoice shall be deemed to be the Statement on the Transfer and Acceptance of the Services.

6.2.3.Upon provision of the Services by the Provider, the Buyer shall check them and must:

6.2.3.1. Not later than within 5 (five) workings days from the actual provision of the Services and the submission of the Statement on the Transfer and Acceptance of the Services, accept the Service result by signing the Statement on the Transfer and Acceptance of the Services; or

6.2.3.2. Accept the Service result with reservations by signing the Statement on the Transfer and Acceptance of the Services and the Defect Report produced during check of the Services where the Buyer must indicate defects in the Services or shortcomings in the documents provided by the Provider, which were noticed during the acceptance process of the Services and set forth the procedure for eliminating those defects or shortcomings (hereinafter referred to as the **Defect Report**); or

Refuse to accept the Service result and to hand over (or send) the Defect Report on defective Services or part thereof to the Provider.

6.2.4.The Statement on the Transfer and Acceptance of the Services shall specify the date on which the Provider provided the Services and all the necessary documents.

6.2.5.If defects in the Services are identified, which cannot be considered as non-compliance with the requirements set out in the Contract, and their elimination does not prevent the Buyer from using the Service result for the intended purpose, the Buyer may accept the Services with reservations, produce a Defect Report and set reasonable time limits for the Provider to eliminate defects in the Services. The Provider shall eliminate defects in the Services within reasonable term limits specified by the Buyer in accordance with Section 7.3 of the General Conditions 'Elimination of defects in the Services'. If the Provider misses time limits for the elimination of defects in the Services, the provisions of Section 7.4 of the General Conditions 'Buyer's rights in case the Provider did not eliminate defects in the Services' shall apply.

6.2.6.If the Buyer fails to submit (send) the Defect Report to the Provider within 5 (five) working days from receipt of the Statement on the Transfer and Acceptance of the Services, it shall be deemed that the Buyer has accepted the Services and has no claims against them.

6.2.7.The risk of loss or damage, or accidental destruction of the products related to the Services shall pass to the Buyer from to the Provider at the moment of actual acceptance of the Services.

6.2.8.The Buyer shall have the right to use the Service result only after signing the Statement on the Transfer and Acceptance of the Services.

6.2.9. If the Provider has provided the Services prior to the deadline specified in the Special Conditions for the provision of the Services but they have defects, and the Provider has failed to eliminate these defects by the deadline for the provision of the Services specified in the Special Conditions, the Provider shall be subject to penalty charges specified in the Special Conditions until the date of provision of the adequate Services.

6.3. Transfer and acceptance of the Services provided in phases

6.3.1. The Provider must provide the Services and transfer the Service result to the Buyer in phases, and the Buyer must accept the good quality Services that meet the requirements of the Contract and laws as well as other legal acts provided at a specific phase. The Services shall be provided in phases in accordance with the sequence of phases and deadlines specified in the Special Conditions.
6.3.2.The Service result provided at a specific phase shall be transferred to the Parties by signing the Statement on the Transfer and Acceptance of the Services, which is executed in 2 (two) copies with the same legal effect (except where the Statement on the Transfer and Acceptance of the Services is signed with a secure electronic signature, one for each Party). Where the requirement of a Statement on the Transfer and Acceptance of the Services as a separate document is not mandatory, the Parties shall agree thereon and expressly refer thereto in the Special Conditions: Invoice shall be deemed to be the Statement on the Transfer and Acceptance of the Services.
6.3.3. The Buyer shall sign each Statement on the Transfer and Acceptance of the Services provided that all previous phases have been accepted, unless otherwise specified in the Special Conditions.
6.3.4. After provision of the Services at all phases, i.e. after completion of the Services, a final Statement on the Transfer and Acceptance of the Services shall be signed.
6.3.5.After the Provider has provided the Services at a specific phase, the Buyer shall verify the Service result and must:
6.3.5.1. Not later than within 5 (five) working days from the actual provision of the Services at a specific phase and submission of the Statement on the Transfer and Acceptance of the Services, accept the Service result of a specific phase by signing the Statement on the Transfer and Acceptance of the Services; or
6.3.5.2. Accept the Service result at a specific phase with reservations by signing the Statement on the Transfer and Acceptance of the Services and the Defect Report produced during the check of the Service phase where the Buyer must indicate defects in the Services of a specific phase observed during the Service phase check or shortcomings in the documents provided by the Provider and set forth the procedure for eliminating those defects or shortcomings (hereinafter referred to as the **Defect Report**); or
6.3.5.3. Refuse to accept the Service result of a specific phase and to forward (or send) the Defect Report to the Provider regarding the improperly provided Services of that phase.
6.3.6.The Statement on the Transfer and Acceptance of the Services must specify the date when the Provider provided the Services at a specific stage and all the necessary documents (if applicable).
6.3.7.If defects in the Services are identified, which cannot be considered as non-compliance with the requirements set out in the Contract, the Buyer may accept the Service result of a specific phase with reservations, produce a Defect Report and set reasonable time limits for the Provider to eliminate defects in the Services. The Provider shall eliminate defects in the Services within reasonable term limits specified by the Buyer in accordance with Section 7.3 of the General Conditions 'Elimination of defects in the Services'. If the Provider misses time limits for the elimination of defects in the Services, the provisions of Section 7.4 of the General Conditions 'Buyer's rights in case the Provider did not eliminate defects in the Services' shall apply.
6.3.8.If the Buyer fails to submit (send) the Defect Report to the Provider within 5 (five) working days from receipt of the Statement on the Transfer and Acceptance of the Services, it shall be deemed that

the Buyer has accepted the Services at a specific phase and has no claims against them.
6.3.9.The Buyer shall have the right to use the result of the Services provided in phases only after signing the final Statement on the Transfer and Acceptance of the Services, unless otherwise provided in the Special Conditions.
6.3.10. The time limit for the performance of any subsequent phase of the Services related to the provision of the previous phase of the Services shall not be automatically extended when the Buyer does not sign the Statement on the Transfer and Acceptance of the Services of the previous phase due to the fault of the Provider.
6.3.11. If the Provider has provided the Services prior to the deadline specified in the Special Conditions for the provision of the Services at a specific phase but they have defects, and the Provider has failed to eliminate these defects by the deadline for the provision of the Services of a specific phase specified in the Special Conditions, the Provider shall be subject to penalty charges specified in the Special Conditions until the date of provision of the adequate Services.

7. WARRANTY OBLIGATIONS OF THE PROVIDER

7.1. Warranty periods (if applicable)

7.1.1.The Service result shall be subject to the statutory warranty period and/or the warranty period applicable by the Provider, which is specified in the tender bid, Technical Specification or Special Conditions. The warranty period shall start from the day of signing of the Statement on the Transfer and Acceptance of the Services.
7.1.2.Warranty periods shall be suspended for as long as the Buyer is unable to properly use the Service result due to defects identified when the Provider is held responsible for them. If the Buyer is unable to use only a specified part of the Service result due to defects in the Services, the warranty periods shall be suspended only regarding such part.
7.1.3.The Provider shall not be liable for any defects in the Services, which have been caused by improper use or maintenance of the Service result, or for the fault of the Buyer, its staff or third parties provided there is no fault of the Provider for such defects in the Services, improper use or maintenance of the Service result.

7.2. Claims for defects in the Services

7.2.1.Having identified defects in the Services within the warranty periods (if applicable) or at any time throughout the period of the Contract, the Buyer shall, immediately but not later than within 30 (thirty) days and not later than by the end of the warranty period, submit a written claim to the Provider and establish reasonable time limits if they have not been specified in the Special Conditions to eliminate defects in the Services.
7.2.2.The Provider shall eliminate all defects in the Services free of charge when the Provider is held liable for such defects within reasonable time limits set in the Buyer’s claim, which are calculated from the date of receipt of the claim, unless specific time limits have been set in the Special Conditions.
7.2.3. If the Provider does not agree with defects in the Services, each of the Parties may call upon an independent expert report. If the Provider, for more than 10 (ten) days from the Buyer’s request, does not respond or does not invite an independent expert who has been agreed with the Buyer to solve the

dispute (the Buyer cannot unreasonably withhold its consent to use the expert proposed by the Provider), or/and if the dispute has lasted longer than 30 days from the Buyer's first request), the Buyer shall have the right to independently call for an expert report. In this case, the costs of the independent expert report shall be borne:

7.2.3.1. By the Buyer if the Service result meets the requirements specified in the Contract as well as in laws and other legal acts;

7.2.3.2. By the Provider if the Service result does not meet the requirements specified in the Contract as well as in laws and other legal acts.

7.2.4. Conclusions of the expert report shall be binding on the Parties.

7.2.5. The Buyer shall not lose the right to claim for defects in the Services, and the Provider shall have the duty to eliminate all defects in the Services free of charge regardless of whether those defects may have been identified at the time of signing the Statement on the Transfer and Acceptance of the Services.

7.3. Elimination of defects in the Services

7.3.1.The Provider must eliminate the defects in the Service result free of charge. If defects in the products relating to the Services have been identified, the Provider must remedy these defects by repairing the products or parts thereof, or by replacing the product with a new product or part thereof.

7.3.2.The Buyer must provide access to the Provider to eliminate defects in the Services, enabling the Provider to do that within the specified time limits. If defects in the products relating to the Service provision are eliminated at the place of use of the products, the Buyer and the Provider must agree on the time for elimination of defects in the products.

7.3.3.If defects in the products relating to the Service provision are repeatedly identified in the repaired part thereof, the Provider shall replace them with new good quality products unless the Buyer agrees in writing with further repair of the products.

7.3.4.After defects in the Service result have been eliminated, the warranty period for the Service result (or for the repaired or new products or parts thereof relating to the Services) shall start to run again from the date, on which the properly provided Services (or products relating to the Services) have been transferred to the Buyer.

7.3.5.If the elimination of defects in the result of the part of the Services affects other parts of the Services, the Buyer may require the Provider to perform repeated tests, which have been performed under the Contract (if any). The Buyer must submit such a written claim to the Provider within 30 (thirty) days after the elimination of defects. Such tests shall be performed in accordance with the terms and conditions of the previous tests except that in all cases they are performed at the risk and at the expense of the Provider.

7.3.6.Having eliminated all defects in the Services, the Provider must inform the Buyer thereof.

7.3.7.Within 5 (five) working days after receipt of the Provider's notification of the elimination of defects in the Services, the Buyer must check the defects specified in the Defect Report or in the Buyer's claim and confirm in writing, which defects in the Services have been eliminated properly.

7.4. The Buyer's rights in case the Provider did not eliminate defects in the Services

7.4.1.If the Provider refuses to eliminate or does not eliminate defects in the Services within reasonable

time limits set by the Buyer, the Buyer shall have the right to:
7.4.1.1. Eliminate defects in the Services either by itself or by hiring third parties and inform the Provider thereof in advance, and to demand that the Provider reimbursed the costs of the expert report and elimination of defects in the Services as well as covered the losses incurred; or
Demand that the Provider reduced the amount due and refunded the overpayment resulting from this reduction within 30 (thirty) days from the deadline set for the Provider to eliminate the defects in the Services if this is not contrary to the principles of the Law on Public Procurement; or
7.4.1.3. Refuse the Services and not pay for such Services or claim for repayment of the amount paid for the Services and terminate the Contract.
7.4.2.The amount payable to the Provider under the Contract shall be reduced to the extent equivalent to the decrease in value of the Services for the Buyer due to the inadequate result of the part of the Services or defects in the products relating to the provision of the Services if value of such result of the part of the Services and/or value of the products might be deducted from the total value of the Services. The decrease in value of the Services shall include, among other things, the Buyer's costs for the identification and elimination of defects in the part of the Services and/or the products (if the price of the part of such Services and/or products was indicated at the time of procurement).
7.4.3.The Provider shall be obliged to pay a monetary claim of the Buyer in accordance with point 7.4.4 of the General Conditions within 30 (thirty) days or within a longer reasonable period specified in the Buyer's claim.
7.4.4.The Buyer shall require the Provider to pay penalty charges specified in the Special Conditions for the delay in the elimination of defects in the Services.

8. TIME LIMITS FOR THE PROVISION OF THE SERVICES

8.1. Time limits for the provision of the Services and provision schedule

8.1.1.The Provider must provide the Services in accordance with the time limits specified in the Special Conditions.
8.1.2.If applicable, the Buyer shall plan a provision schedule of the Services and submit it to the Provider for agreement (hereinafter referred to as the **Schedule**) not later than within 14 (fourteen) working days from the entry into force of the Contract or within another time limit specified in the Procurement documents.
8.1.3.If relevant, the Schedule must indicate, which Services can be provided in parallel, and which can only be provided in the established order of priority.

8.2. Penalty charges for delays in providing the Services

8.2.1. If the Provider misses time limits for the provision of the Services set out in the Special Conditions, it shall be subject to penalty charges specified in the Special Conditions until the date of the provision of the Services.
8.2.2. If the Provider misses the time limit for the provision of the Services or their phase, penalty charges shall be calculated from the deadline of the provision of the Services or their phase (not inclusive) until the date of the provision of the Services or their phase (inclusive) determined in accordance with the Statements on the Transfer and Acceptance of the Services.

8.2.3. If the Provider has been imposed penalty charges under this Contract, the amount payable by the Buyer for the Services shall be reduced by the amount of accrued penalty charges. The Buyer shall also have the right to unilaterally deduct penalty charges from any amounts payable to the Provider in accordance with the procedure established by legal acts, notifying the Provider in writing about the deduction of such penalty charges.

9. MEANS OF SECURING THE DISCHARGE OF CONTRACTUAL OBLIGATIONS

The discharge of contractual obligations of the Parties shall be secured by the means of securing the discharge of contractual obligations specified in Section 8 of the Special Conditions, the procedure for securing the performance of contractual obligations set out in Section 10 of the General Conditions, the advance security specified in point 12.1.3 of the General Conditions (if the Special Conditions establish the amount of the advance and require the advance security), penalty charges specified in Section 9 of the Special Conditions.

10. PERFORMANCE SECURITY (IF APPLICABLE)

10.1. The provisions of this Section shall apply if the Special Conditions establish that the Provide must forward the first demand bank guarantee or a suretyship bond of the insurance company or other performance security specified in the Special Conditions to ensure the proper performance of the Contract.

Note: Where the Special Conditions state that the Buyer requires a performance security issued by a credit union, the provisions of this Section shall apply depending on the need, and the Buyer may include additional requirements complying with the provisions of laws and other legal acts in the Special Conditions for the provision of such performance security.

10.2. The Provider must provide the Buyer with the performance security, which type and amount is established in the Special Conditions: the first demand bank guarantee or the suretyship bond of the insurance company (the suretyship bond of the insurance company must be accompanied by the signed insurance certificate (policy) and a document proving that the insurance premium for the issued **suretyship** bond has been paid), complying with the conditions specified in Section 10 of the Special Conditions within the time limit specified in the Special Conditions (hereinafter referred to as the **Performance Security**).

10.3. If the Provider does not provide the Buyer with the Performance Security of the amount specified in the Contract within the time limit set therein, the Provider shall be deemed to have refused to conclude the Contract and the Buyer shall have the right to propose the Contract to another Provider in accordance with the procedure provided for in the Law on Public Procurement.

10.4. Before providing the Performance Security, the Provider may request the Buyer to confirm that the Buyer agrees to accept the Provider's proposed Performance Security. In this case, the Buyer must reply to the Provider not later than within 3 (three) working days from the date of receipt of the Provider's request.

10.5. A bank (insurance company) must include irrevocable and unconditional commitment in the Performance Security to pay the Buyer the amount specified in the Performance Security by transferring the money to the Buyer's account not later than within 15 (fifteen) days from the date of receipt of the

Buyer's written notification of the Provider's breach of obligations under the Contract, partial or total failure to perform these obligations or their improper performance.

10.6. The Performance Security may not state that the bank (insurance company) is responsible only for the direct loss compensation. The bank (insurance company) does not have the right to demand the Buyer to justify its claim. The Buyer shall indicate in the notice to the bank (insurance company) that the amount of Performance Security is due because the Provider has partially or completely failed to perform the Contract and/or it has been terminated due to the fault of the Provider. The Buyer shall not undertake to prove the actual losses incurred, and the Provider confirms by signing the Contract and providing the Performance Security that the amount of the Performance Security is considered to be minimum losses of the Buyer that do not need to be justified.

10.7. The Performance Security shall take effect not later than the date of its submission to the Buyer.

10.8. The amount of the Performance Security shall be quoted and paid in euro.

10.9. The Performance Security must be in Lithuanian or another language (a translation into Lithuanian must be provided if the Buyer requests it).

10.10. The term of validity specified in the Performance Security shall be not less than the term of validity specified in the Special Conditions.

10.11. If the duration of the Contract is longer than 1 (one) year, the Provider shall have the right to provide a Performance Security valid for 1 (one) year; however, the Provider must extend the term of the Performance Security or provide a new Performance Security thereafter not later than 10 (ten) working days before the expiry of the Performance Security.

10.12. In case the time limit for the provision of the Services is extended under the conditions laid down in the Contract or is postponed due to the suspension thereof, or the provision of the Services or the elimination of defects in the Services is delayed, the Provider shall ensure validity of the Performance Security for the entire period of the Contract and shall provide the Buyer with a new or extended Performance Security not later than by the end of validity of the Performance Security.

10.13. If the Provider fails to extend the Performance Security or fails to provide a new Performance Security in a timely manner, the Buyer shall have the right to demand penalty charges specified in the Special Conditions for each day of delay.

10.14. The Buyer shall not accept the Performance Security and/or consider it invalid, and/or shall request the Provider to provide a new Performance Security to the Buyer; whereas the Provider must provide the Performance Security within the shortest possible period if the Performance Security does not meet the requirements of the Contract, or the Buyer has information related to the suspension or possible suspension of the activities of the bank (insurance company) that issued the Performance Security (including insolvency, liquidation or imposition of legal protection procedures).

10.15. If the Provider violates the obligations set out in the Contract, partially or completely fails to discharge the obligations (or performs them outside the terms and conditions of the Contract), the Buyer may use the Performance Security. To continue with the discharge of contractual obligations, the Provider must provide the Buyer with a new Performance Security, which amount is specified in the Special Conditions, within 10 (ten) working days from the date of receipt of the notification regarding payment of the Performance Security to the Buyer.

10.16. The Buyer may use the Performance Security in any of the following circumstances:

10.16.1. The Provider has failed to discharge its contractual obligations; it does not perform or inadequately performs its contractual obligations;

10.16.2. The Provider fails to comply with the Buyer's demand to eliminate defects in the Services within a reasonable time limit;
10.16.3. If the Buyer has suffered losses (including but not limited to additional costs, income foregone or other direct and indirect damages, default interest and/or penalties (if default interest and/or penalties are provided for in the Special Conditions of the Contract) due to any actions of the Provider (acts or omissions);
10.16.4. The Provider unilaterally terminates the Contract without any valid reason (not in cases specified in the Contract).

11. CONTRACT PRICE AND ITS RECALCULATION

11.1. The Contract price, which the Buyer must pay to the Provider for the Services actually provided under the terms and conditions of the Contract, including all Arrangements, shall be calculated using the method or methods of calculating the price specified in the Special Conditions.
11.2. Initial Contract Value shall be specified in the Special Conditions.
11.3. The Contract price shall be deemed to include all costs incurred by the Provider in connection with the provision of all Services as well as with the proper discharge of the Provider's other contractual obligations, including insurances, customs duties and other expenses incurred by the Provider when performing the contractual obligations.
11.4. The Contract price shall be reviewed in accordance with the procedure laid down in the Special Conditions.

12. PAYMENT PROCEDURE

12.1.Advance payment (an advance) (if applicable)

12.1.1. The provisions of Section 12.1 of the General Conditions shall apply if the Special Conditions state that an advance payment (an advance) is paid to the Provider (hereinafter referred to as the Advance).
12.1.2. The Buyer shall pay the Provider an Advance not exceeding the amount specified in the Special Conditions.
12.1.3. Where required by the Special Conditions, in order to receive an Advance and when applying for the payment thereof, the Provider shall submit the proforma invoice to the Buyer accompanied by an **Advance** security, i.e. a bank guarantee or a suretyship bond of the insurance company or any other performance security, which amount is not less than the Advance stated in the Special Conditions, (hereinafter referred to as the **Advance Security**) not later than within 10 (ten) working days from the date of entry into force of the Contract.
Note: Where the Special Conditions state that the Buyer requires an Advance Security issued by a credit union, the provisions of this Section shall apply depending on the need, and the Buyer may include additional requirements complying with the provisions of laws and other legal acts in the Special Conditions for the provision of such Advance Security.
12.1.4. Before providing the Advance Security, the Provider may request the Buyer to confirm that the Buyer agrees to accept the Provider's proposed Advance Security. In this case, the Buyer must reply to

the Provider not later than within 3 (three) working days from the date of receipt of the Provider's request.

12.1.5. A bank (insurance company) must include irrevocable and unconditional commitment in the Advance Security to pay the Buyer the amount not exceeding the amount of the Advance paid and the Security amount by transferring the money to the Buyer's account not later than within 15 (fifteen) days from the date of receipt of the Buyer's written notification of non-performance of the Contract or termination thereof due to the fault of the Provider.

12.1.6. The bank (insurance company) does not have the right to demand the Buyer to justify its claim. The Buyer shall indicate in the notice to the bank (insurance company) that the amount of Advance Security is due because the Provider has partially or completely failed to perform the Contract and/or it has been terminated due to the fault of the Provider, and the Provider did not repay the advance.

12.1.7. The amount of the Advance Security shall be quoted and paid in euro.

12.1.8. The Advance Security must be in Lithuanian or another language (a translation into Lithuanian must be provided if the Buyer requests it).

12.1.9. The Advance Security that does not meet the requirements set out in this Section of the Contract shall not be accepted.

12.1.10. If the bank (insurance company) that issued the Advance Security is unable to discharge its obligations during the performance of the Contract, the Buyer may send a written demand to the Provider to provide a new Advance Security within 10 (ten) working days under the same conditions as the previous one.

12.1.11. The Buyer shall pay the Provider an Advance within the period provided for in the Special Conditions from the date of receipt of the proforma invoice and Advance Security (if applicable). The amount of the Advance paid shall be deducted from the amount due.

12.1.12. Upon termination of the Contract, the Provider must refund the received Advance to the Buyer within 5 (five) working days (if part of the Services has been already provided and the Buyer has accepted them and can use the Service result for its purpose, the part of Advance shall be refunded, which exceeds the price of the Services accepted by the Buyer). If the Provider fails to repay the received Advance, the Buyer shall use the Advance Security (if applicable). In cases where Point 12.1.3 of the General Conditions was not applied, the Provider shall pay penalty charges specified in the Special Conditions on the amount of Advance to be repaid for the period from the date of Advance payment until its repayment.

12.2. Payment arrangements

12.2.1. The Provider shall issue an Invoice only after the Parties have signed the Statement on the Transfer and Acceptance of the Services unless otherwise provided in the Special Conditions:

12.2.1.1. Electronic invoice that complies with the European standard for electronic invoices, the reference of which was published in the Commission Implementing Decision (EU) 2017/1870 of 16 October 2017 on the publication of the reference of the European standard on electronic invoicing and the list of its syntaxes pursuant to Directive 2014/55/EU of the European Parliament and of the Council (hereinafter referred to as the **European e-Invoicing Standards**) shall be submitted by means selected by the Provider.

12.2.1.2. The Provider may submit an electronic invoice not complying with the European e-Invoicing Standard only using the tools of the General Information System of Invoice Administration (hereinafter

referred to as the SABIS).
12.2.2. The Buyer shall accept and process electronic invoices using tools of the information system SABIS, except, when in case of mobilisation, war or emergency, there are damages of the SABIS, which prevent communication and exchange of information between the Buyer and the Provider using the SABIS.
12.2.3. The Provider must submit the proforma invoices (if the Special Conditions provide for the Advance payment) in accordance with the procedure set out in this Section of the Contract.
12.2.4. The Buyer shall pay for the Services within the time limits set forth in the Special Conditions.
12.2.5. The Buyer shall be subject to the penalty charges in accordance with the procedure laid down in the Special Conditions for delays in payments under the Contract.
12.2.6. If the Services are provided in phases or periods, the said payment arrangements shall be applicable for each phase or period of the Service provision, unless otherwise specified in the Special Conditions.
12.2.7. If the Parties enter into a tripartite agreement with the sub-provider regarding direct payment, the Buyer shall transfer the amount due to the sub-provider to the sub-provider's bank account specified in the tripartite agreement and transfer the balance to the Provider's bank account after the Statement on the Transfer and Acceptance of the Services provided is concluded in accordance with the requirements of the Contract and the tripartite agreement and the Provider sends the invoice for the Services to the Buyer.

12.3. Other payment issues

12.3.1. The Buyer must transfer payments to the Provider to the bank account of the Provider specified in the Special Conditions.
12.3.2. The Buyer shall have the right to deduct the amounts receivable from the Provider from payments to the Provider under the Contract (to make unilaterally offsetting). For this reason, the Provider shall not be entitled to transfer or pledge the rights of claim in respect of receivables under the Contract to third parties or otherwise dispose of them without the consent of the Buyer.
12.3.3. All payments under the Contract shall be made in euro.
12.3.4. The Party being late with the due payments under the Contract must pay the other Party penalty charges specified in the Special Conditions.

13. CONFIDENTIAL INFORMATION

13.1. The Parties undertake to respect confidentiality and, without a written consent of the other Party, not to disclose the information of that Party indicated as confidential to any employees of the Party, to any third parties associated with the Party, or to any other third parties who do not need to use this information for their business purposes, except in the cases specified below.
13.2. A Party shall have the right to disclose confidential information of the other Party in the following cases:
13.2.1. Disclosure of confidential information is necessary for the proper performance of contractual rights or obligations of the Party; however, in such case, the information may be disclosed only to the extent necessary for the performance of contractual rights or obligations and only to such third parties whom this information is necessary, provided that third parties receiving confidential information

assume the same confidentiality obligations as those laid down in this Contract. If third parties disclose confidential information, the Party shall be responsible for their actions as for its own;
13.2.2. Confidential information must be disclosed in accordance with the requirements of laws and other legal acts, including cases when required by entities of public administration, as defined in the Law on Public Administration of the Republic of Lithuania.
13.3. Before disclosing confidential information, the Party must inform the other Party (in so far as this is not prohibited by laws or other legal acts) of the necessity or the requirement received from the entity of public administration to disclose confidential information and take reasonable measures to ensure the confidentiality of the disclosed information.
13.4. The Party shall be held liable for:
13.4.1. Any unlawful, including accidental, disclosure or transmission of confidential information or any part thereof of the other Party, or unlawful use of confidential information;
13.4.2. Failure to take all reasonable steps and actions to preserve and protect confidential information of the other Party or any part thereof, to prevent its further unlawful disclosure, transfer or use.
13.5. In the event of unjustified disclosure of confidential information of the other Party, the Party shall be liable to pay the other Party a fine, which amount is specified in the Special Conditions.

14. PROTECTION OF PERSONAL DATA

14.1. The Parties undertake to ensure the security of personal data and the lawful processing of personal data in accordance with the provisions of 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) and other legal acts governing the processing of personal data.
14.2. The Parties shall confirm that, if personal data is processed in to ensure the proper performance of the Contract, the Parties undertake to conclude a separate arrangement on the processing of data, which determines the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the data controller.

15. INTELLECTUAL PROPERTY

15.1. All the results and related rights acquired in the course of the performance of the Contract, including intellectual property rights, except for personal non-property rights to intellectual property results, shall be the property of the Buyer, which is transferred to the Buyer from the signature of the Statement on the Transfer and Acceptance of the Services without any reservation, which the Buyer may use, publish, convey or transfer to third parties without the explicit consent of the Provider unless the Special Conditions provide for otherwise, or intellectual property rights may not be transferred into ownership because of the nature of the Services or/and exclusive rights, patents etc.
15.2. The Provider undertakes to indemnify the Buyer for any claims arising from intellectual property rights, including, but not limited to, patent, trademark, the right (registered or not) of industrial design owner (user), the right arising from applications for the registration of any of the said rights, copyright, the (sui generis) right of database manufacturers, names of firms, companies, organisations, businesses or name owners and other similar rights or obligations regardless of their registration in the Republic

of the Republic of Lithuania or in other countries, or non-registration, except for cases when such breach is caused by the Buyer's fault.

15.3. The Provider shall not have the right to use the Buyer's symbols, name and trademark in advertising, marketing without a prior written consent of the Buyer, as well as to use results of intellectual activities produced by the Buyer. In case of violation of the requirement, the Provider shall be subject to the fine specified in the Special Conditions.

16. DECLARATIONS AND GUARANTEES

16.1. Each Party shall declare and guarantee to the other Party that:

16.1.1. All necessary decisions have been legally adopted and are in force; permissions and consents have been obtained; also, other legal actions necessary for the conclusion, validity and performance of the Contract have been legally executed and are valid;

16.1.2. When concluding a Contract, the Party shall not exceed its competence and shall not violate the applicable laws and other legal acts, decisions of a court or arbitration court, administrative acts, contracts or other obligations under applicable private law, public law, the European Union law or international law;

16.1.3. A representative of the Party has all the necessary powers to conclude and perform the Contract. When concluding and signing the Contract, a representative of the Party does not violate the Articles of Association, regulations and other internal documents of thereof, the rights and legitimate interests of the Party's management and other bodies and/or creditors; when concluding the Contract, it is acting in good faith and reasonable manner with regard to the members of the Party and bodies of the Party and creditors;

16.1.4. The Party has assessed all circumstances, which are essential for the conclusion and performance of the Contract. None of the conditions and circumstances specified in the Contract adversely affect the Party's will to conclude the Contract under the terms and conditions specified therein, and to discharge the obligations arising from the Contract;

16.1.5. The Contract is concluded in accordance with the principles of good faiths, reasonableness, justice and equality of Parties, without the use of deception or pressure. The Parties have disclosed to each other all information, which is of fundamental importance for the conclusion and performance of the Contract;

16.1.6. All declarations and guarantees of the Party are comprehensive and do not leave behind any circumstances that would make these declarations or guarantees false.

16.2. The Provider shall additionally declare and guarantee to the Buyer that the Provider, sub-providers, joint venture partners and specialists have all valid and lawful permits, licences, certificates, attestation documents provided for in laws and other legal acts, which are required for the performance of the Contract.

16.3. The Provider shall declare that the rights of disposal, management and use of the Service result provided are not limited, and no third parties have any claims to the Service result transferred under the Contract.

16.4. When performing the Contract, the Provider undertakes to comply with the obligations of environmental, social and labour law laid down in European Union and national law, collective agreements and international conventions referred to in Annex 5 to the Law on Public Procurement.

17. GENERAL LIABILITY ISSUES

17.1. Payment of penalty charges for delay or breach of the contractual obligations shall not exempt a Party from the performance of its obligations under the Contract.
17.2. Payment of penalty charges and/or the receipt of the Performance Security shall not deprive the Party of the right to demand the other Party to compensate for the losses incurred by it. The penalty charges provided for in this Contract shall be deemed to be minimal losses of the Parties that do not need to be justified. Each of the Parties shall be entitled to receive indemnity from the other Party for the improper performance or non-performance of contractual obligations of the other Party, up to the Initial Contract Value, unless the legislation provides for a higher amount to be reimbursed. The limitation of liability provided for in this point shall not apply if the damage is caused by breach of confidentiality obligations, personal data protection legislation or intellectual property rights.
17.3. In the event any of the declarations or guarantees provided in this Contract prove to be substantially incorrect, false or misleading, the Party committing a breach shall be liable to the injured Party for any loss suffered by the injured Party as a result of such incorrect, false or misleading declaration or guarantee.
17.4. The legal remedies provided for in this Contract shall not restrict the Parties' right to use other legal remedies.
17.5. The limitations of liability under the Contract shall be not applicable where the damage is caused intentionally or by gross negligence, also where non-material damage, health injury or death is suffered, as well as damage (loss) to third parties is caused, including cases where the damage caused by one Party to third parties is compensated by another Party.
17.6. Upon expiry of the Contract, the Parties shall not be exempt from liability for breach of the Contract. Upon expiry of the Contract, the Parties shall not lose the right to claim compensation for losses incurred due to the failure to perform the Contract and to pay penalty charges.

18. FORCE MAJEURE

18.1. Liability under the Contract shall not be applicable, and the Parties may be released from civil liability in whole or in part on the following grounds:
18.1.1. In the event of *force majeure*: the provisions of the Article 6.212 of the Civil Code of the Republic of Lithuania and the Rules approved by Resolution No 840 of the Government of the Republic of Lithuania of 15 July 1996 On the Approval of the Rules of Release from Liability in the Event of *Force Majeure* shall apply;
18.1.2. Because of the actions taken by the Member States of the European Union: where the obligation under the Contract cannot be fulfilled due to the mandatory and unforeseen actions (acts) of the public authorities of the European Union, which the Parties were not entitled to challenge and could not have been foreseen in advance.
18.2. A Party seeking release from liability must notify the other Party of *force majeure* circumstances immediately but not later than within 5 (five) days of the occurrence or discovery of such circumstances, providing evidence that it has taken all reasonable precautions and has made every effort to reduce costs or negative consequences, as well as to notify of the possible deadline for the discharge of obligations. The Party shall also provide the other Party with appropriate notice when the grounds for non-performance of the obligations cease to exist.

18.3. The grounds for releasing any Party from the obligations shall arise from the moment when the *force majeure* occurs or, if no notification was sent in due time, from the moment of sending a notification. If any Party fails to send the notification or fails to inform the other Party in due time, it must compensate the other Party for the damage caused by the failure to provide the notification in due time or the fact that no notification has been sent.
18.4. If *force majeure* circumstances persist for more than 1 (one) month from the date of receipt of the notification, either Party may terminate the Contract by notifying the other Party 5 (five) working days prior to such termination. *Force majeure* shall not be considered the circumstances when the Party does not have the necessary financial resources, or the debtor's counterparties violate their obligations, or the debtor violates its obligations to counterparties.

19. INVALIDITY OF THE PROVISIONS OF THE CONTRACT

19.1. If any provision of the Contract is or becomes invalid, whether in full or in part, the Parties shall conclude an Arrangement as soon as possible and replace the invalid provision with another provision which, as far as possible, would have the same economic and legal effect as was sought in the event of the agreement on the invalid provision of the Contract. Such an invalid provision shall not invalidate other provisions of the Contract provided this does not violate laws and other legal acts, and it may be assumed that the Contract would have been lawfully concluded and without inclusion of the invalid provision.
19.2. If the amendment of the General Conditions provided for in the Special Conditions is or becomes invalid, whether in full or in part, the version of the General Conditions prior to the amendment may not be applicable. In such a case, the Parties shall act in accordance with point 19.1 of the General Conditions.

20. AMENDMENTS TO THE CONTRACT

20.1. Conditions of the Contract may not be changed during the term of the Contract, except for those conditions, the amendment of which is provided for in the Contract and/or is possible in accordance with the provisions of the Law on the Public Procurement.
20.2. Amendments to the Contract shall be made by concluding an Arrangement between the Parties.
20.3. The Party, initiating the Arrangement, shall send a notice of amendment to the Contract to the other Party and a justification for the existence of an actual and legal basis for concluding the Arrangement. The other Party must analyse and evaluate the received information within 5 (five) working days (or within another time limit agreed in writing by the Parties), submit their comments and proposals based on the provisions of the Contract and mandatory provisions of laws and other legal acts.
20.4. An Arrangement shall enter into force from the date of its conclusion unless otherwise specified in the Contract. The Buyer must make the Arrangement public in accordance with the procedure laid down in Articles 33 and 86 of the Law on Public Procurement.
20.5. Changes in the contact details and details of entities specified in the Special Conditions shall not be considered as an amendment to the Contract (except for the replacement of the Provider, joint venture partner, sub-provider or specialist), and the Party shall change those details unilaterally by informing the other Party thereof. In any event, the amendment to the Contract may not substantially

alter the Contract.

21. SUSPENSION OF THE CONTRACT

21.1. In the absence of fault of the Provider, and in the event of circumstances, which the Party to the Contract could not foresee when concluding the Contract and which prevent the Party from discharging its contractual obligations, and/or in the event of other unforeseen circumstances, the Parties to the Contract shall be entitled to initiate the suspension of provision of the Services (part of them) until the relevant circumstances cease to exist.
21.2. Provision of the Services (part of them) may be suspended if any of the following conditions occurs:
21.2.1. In the *force majeure* circumstances provided for in Section 18 of the General Conditions, the time limits for discharge of the contractual obligations shall be suspended from the moment the obstacle appears, or, if it has not been notified in a timely manner, from the moment of notification, and they shall be updated when the said circumstances no longer prevent the performance of the Contract;
21.2.2. The Provider may not provide the Services in accordance with the procedure specified in the Contract (e.g., the Buyer cannot ensure technical capacities for the provision of the Services for objective reasons), and the Provider is, therefore, unable to perform the Contract;
21.2.3. Due to procurement of unforeseen products, services and/or works related to the Procurement object, the need of which became apparent only during the performance of the Contract;
21.2.4. The performance of another procurement contract of the Buyer that directly affects this Contract is delayed without any fault on the Buyer's part;
21.2.5. In the event of evidence-based barriers or obstacles caused to the Provider by other third parties not by the reason of the Provider's contractual obligations, which have not been performed in a timely or proper manner in accordance with the conditions and procedures of the Contract;
21.2.6. In the event of amendments to the applicable legal act, or upon the entry into force of a new legal act, which affects the performance of this Contract;
21.2.7. The need to suspend the contractual obligations arose due to suspended, redistributed, unreceived, etc. funds allocated by the Buyer for the procurement of the Services or a lack of funding;
21.2.8. Due to judicial (arbitration) disputes with the Buyer or third parties, the subject-matter of which is directly related to the performance of the Contract.
21.3. Where the suspension of provision of the Services (the part thereof) is caused by the circumstances specified in point 21.2 of the General Conditions and lasts not more than 3 (three) months, such suspension shall be deemed to be an amendment to the Contract under the terms and conditions laid down therein and shall be documented following the procedure provided for in point 21.6 of the Contract.
21.4. Where provision of the Services (the part thereof) is suspended due to the circumstances other than those mentioned in point 21.2 of the General Conditions, or/and the circumstances specified in point 21.2 of the General Conditions continue for more than 3 (three) months, and/or are outside the procedure laid down in this Section, it shall be considered as an amendment to the Contract that must be executed in accordance with the provisions of the Law on the Public Procurement and documented following the procedure provided for in point 21.6 of the Contract.
21.5. Performance of contractual obligations may be suspended only during the term of the Contract under the following procedure:

21.5.1. In the event of circumstances that prevent the Provider from discharging its contractual obligations, the Provider shall immediately inform the Buyer thereof. The Provider in its written request must describe the circumstance of suspension (point 21.2 of the General Conditions) and provide arguments, objective facts and evidence supporting the occurrence of such circumstance and possible duration. The Buyer, having assessed the request, shall inform the Provider in writing within 3 (three) working days of the decision taken regarding the suspension of contractual obligations. If the Provider fails to provide specific arguments, facts based on evidence, the Buyer shall have the right to send a written refusal to suspend the contractual obligations.
21.5.2. After the Buyer has informed the Provider in writing and provided a reasoned explanation of the circumstances and the term necessary to suspend the performance of the contractual obligations, the Provider shall inform the Buyer and confirm its agreement with the suspension in writing not later than within 3 (three) working days. The Provider shall have the right to object to the suspension of contractual obligations only if the Provider is able to eliminate, at its own expense and on its own, the circumstances, which led to the necessity to suspend the performance of the contractual obligations.
21.5.3. Upon receipt of a written notice of the Buyer about the suspension, the Provider shall immediately but not later than within 3 (three) working days after the date of sending the confirmation to the Buyer suspend the performance of the contractual obligations or part thereof. If the performance of contractual obligations or part thereof has been suspended, the Parties may not fulfil any of the obligations assigned to them under the Contract or part of the Contract.
21.6. The Parties shall formalise suspension of the performance of contractual obligations by means of a written Arrangement, describe reasons and set the term of suspension, as well as enclose documents confirming the grounds for suspension; the Arrangement shall be signed by the representatives authorised by the Parties. Such Arrangements shall become an integral part of the Contract.
21.7. The performance of contractual obligations shall be suspended for no longer than the duration of a specific, justified circumstance.
21.8. The Parties shall agree that the suspension term of contractual obligations is not included in the performance term of the Contract; the contractual obligations shall not be fulfilled during that term, and the Buyer shall not make any payments, pay fines or reimburse for downtime to the Provider.
21.9. If time limits for the performance of contractual obligations have been suspended on the grounds laid down in the Contract, they shall be updated after extinction of the circumstances, which led to the suspension, or after the term specified in the Arrangement between the Parties, whichever is earlier. In the event the time limits for performance of obligations provided for in the Contract are renewed before expiry of the suspension period specified in the Arrangement between the Parties, the Parties shall document the date of renewal of the time limits for performance of obligations provided for in the Contract in writing.
21.10. After renewal of the performance of the Contract, time limits for the performance of outstanding obligations (part of them) and validity of the Contract shall be extended for the period remaining for their performance (validity of the Contract) at the time of their suspension.
21.11. If the performance of contractual obligations has been suspended for a period exceeding 3 (three) months, after that period, a Party may require the other Party to renew the performance of the Contract by sending a written notice. If the Party fails to renew the performance of the Contract without reasonable circumstances within 10 (ten) days from the relevant notice, the other Party may terminate the Contract by giving a notice to the other Party 10 (ten) days prior to such termination.

22. TERMINATION OF THE CONTRACT

The Contract may be terminated in cases provided for in Article 90 of the Law on Public Procurement and in the Contract, including the possibility of termination by the Arrangement between the Parties.

22.1.Claims for breach of the Contract

22.1.1. If the Party breaches the Contract or laws and other legal acts, the other Party shall have the right to make a written claim thereto and specify what provision of the Contract or laws and other legal acts has been violated and in what way the opposite Party has violated it, as well as to set a reasonable time limit for remedy of the breach.
22.1.2. Upon receipt of the claim, the Party must respond thereto without delay but not later than within 5 (five) working days and indicate what measures will be taken to remedy the breach within the time limit set in the claim or to propose another reasonable time limit in a reasoned manner. The right of the Provider to propose another time limit shall not be considered as the Buyer's obligation to accept that time limit. The proposed time limit of the Party who received the claim shall substitute the time limit specified in the claim only if it is approved by the other Party.

22.2.Termination of the Contract at the initiative of the Buyer

22.2.1. The Buyer shall terminate the Contract unilaterally by notifying the Provider in writing at least 5 (five) days prior to such termination if the Provider commits a material breach of the Contract specified in the Special Conditions, or breach of the Contract, which has features of the material breach of the Contract specified in the Civil Code of the Republic of Lithuania and, upon receipt of the Buyer's claim, fails to remedy the breach within the time limit specified in the claim.
22.2.2. The Buyer shall have the right to terminate the Contract or part thereof unilaterally by sending a written notice to the Provider at least 10 (ten) days prior to such termination if:
22.2.2.1. The Provider is subject to insolvency proceedings or out-of-court bankruptcy proceedings, they become insolvent or there is a probability of insolvency, they suspend economic activity or when a similar situation arises in accordance with the procedure laid down in laws and other legal acts;
22.2.2.2. The Provider's situation changes, and it meets grounds for exclusion laid down in the Procurement documents;
22.2.2.3. Legal acts related to the subject matter of the Contract, the performance thereof, or the activities performed by the Buyer regarding which the Contract has been concluded, change and, as a result, the Buyer decides to terminate the Contract;
22.2.2.4. The Buyer decides to stop the activities, which require the Services procured under the Contract; therefore, the need for the Contract disappears;
22.2.2.5. The governing body of the Buyer makes a decision and the need for the Contract disappears as a result;
22.2.2.6. The Buyer's financial situation changes (get worse), or the Buyer does not receive or loses financing and, therefore, decides to terminate the Contract;
22.2.2.7. There are changes in the organisational structure of the Buyer, i.e. legal status, nature or management structure, and this may affect the proper performance of the Contract or the need for the Contract;

22.2.2.8. There is no need for the Services procured;
22.2.2.9. The Buyer receives an order or recommendation from the authorities supervising procurements to terminate the Contract;
22.2.2.10. The Provider is late to provide an extension of the Performance Security for more than 10 (ten) working days from the expiry date of the last Performance Security or refuses to provide it;
22.2.2.11. The Provider refuses to eliminate or does not eliminate defects in the Services within reasonable time limits set by the Buyer;
22.2.2.12. The Provider breached the Contract or laws and other legal acts and does not remedy the breach within the time limit specified in the written claim of the Buyer;
22.2.2.13. In accordance with the procedure established by the Law on the Protection of Objects of Importance to Ensuring National Security, the Government of the Republic of Lithuania shall adopt a decision confirming that the Contract does not meet the interests of national security (it is applicable if the Buyer operates in the areas, which are considered a part of economic sector of strategic importance to ensuring national security, or is deemed to be a substantial entity);
22.2.2.14. The circumstances referred to in Articles 37 (8) and/or 47 (8) of the Law on Public Procurement have been identified;
22.2.3. The Contract shall be considered null and void if it is established that the performance of the Contract is in conflict with mandatory international sanctions implemented in the Republic of Lithuania as defined in the Law on International Sanctions and other international legislation, legal acts of the European Union and the Republic of Lithuania (at least to one of the applicable sanctions). The moment of invalidity of the Contract shall be determined in accordance with the said Law.
22.2.4. The Buyer shall immediately but not later than within 5 (five) days terminate the Contract unilaterally or suspend its performance for the period of implementation of mandatory international sanctions as defined in the Law on International Sanctions and other international legislation, legal acts of the European Union and the Republic of Lithuania, by notifying the Provider in writing thereof if the Contract entered into force before the imposition of these international sanctions in the Republic of Lithuania. It shall be forbidden to assume new obligations under the Contract, the performance of which would be contrary to international sanctions implemented in the Republic of Lithuania.
22.2.5. If the Contract is terminated in the event of a material breach thereof by the Provider, or the Provider unreasonably terminates the performance of the Contract in conflict with the procedure laid down therein, and if the Special Conditions do not provide that the proper performance of the Contract is ensured by the Performance Security, the Provider undertakes to pay the Buyer a fine specified in the Special Conditions and to compensate for the losses related to the termination of the Contract. If the Special Conditions provide that the proper performance of the Contract is ensured by the Performance Security, the Provider undertakes to pay the remaining part of the fine specified in the Special Conditions and to compensate the Buyer for the losses related to the termination of the Contract to the extent they are not covered by the Performance Security. If the Buyer claims compensation for the losses incurred, the amount of fine shall be credited with the loss compensation.
22.2.6. The Buyer shall have the right to terminate the Contract unilaterally in other cases specified in the Special Conditions (if applicable) as well as in laws and other legal acts.
22.2.7. The Contract shall be deemed to be terminated on the day following the expiry of the notice period for the termination thereof.
22.2.8. In cases where the Provider remedies the breach, or the circumstances that led to the initiation of the procedure for termination of the Contract no longer prevail, the Contract may not be terminated

and the notice of termination of the Contract shall cease to be valid if the Provider presents information about the breach remedy or extinction of the circumstances that led to the initiation of the procedure for termination of the Contract.

22.3. Termination of the Contract at the initiative of the Provider

22.3.1. The Provider shall have the right to terminate the Contract unilaterally by sending a written notice to the Buyer not less than 30 (thirty) days prior to such termination if the Buyer violates the terms of payment to the Provider (except in cases when the Buyer exercises its right to withhold payments), and the Buyer's debt to the Provider exceeds 20% (twenty) of the Initial Contract Value, and the Buyer does not pay the amounts due to the Provider within 30 (thirty) days upon receipt of the Provider's claim.
22.3.2. The Provider shall have the right to terminate the Contract unilaterally by sending a written notice to the Buyer not less than 10 (ten) days prior to such termination if:
22.3.2.1. The Buyer is subject to insolvency proceedings, out-of-court bankruptcy proceedings, it becomes insolvent or there is a probability of insolvency, the Buyer suspends activities, or a similar situation arise in accordance with the procedure laid down in laws and other legal acts;
22.3.2.2. The Buyer breaches the Contract or laws and other legal acts and does not remedy the breach within the time limit specified in the written claim of the Provider except for the case specified in Point 22.3.1 of the General Conditions.
22.3.3. If the circumstances referred to in point 22.3.1 of the General Conditions relate only to a separate part of the Contract or separate Arrangement, the Provider shall have the right to terminate the Contract only in respect of that part or terminate only such Arrangement.
22.3.4. The Provider shall have the right to terminate the Contract unilaterally in other cases specified in laws and other legal acts.
22.3.5. If the Contract is terminated in the event of a material breach thereof by the Buyer, or the Buyer unreasonably terminates the performance of the Contract in conflict with the procedure laid down therein, the Buyer undertakes to pay the Provider a fine specified in the Special Conditions and to compensate for the losses related to the termination of the Contract.
22.3.6. The Contract shall be deemed to be terminated on the day following the expiry of the notice period for the termination thereof.
22.3.7. In cases where the Buyer remedies the breach within the time limit for notice of termination of the Contract, or the circumstances that led to the initiation of the procedure for termination of the Contract no longer prevail, the Contract may not be terminated and the notice of termination of the Contract shall cease to be valid if the Buyer informs the Provider about the breach remedy or extinction of the circumstances that led to the initiation of the procedure for termination of the Contract.

22.4. Rights and obligations of the Parties in the event of termination of the Contract

22.4.1. Termination of the Contract shall not affect validity of the terms and conditions of the Contract, which determine the dispute settlement procedure, as well as other terms and conditions of the Contract, which, in substance, remain valid after termination thereof.
22.4.2. Upon termination of the Contract, the Parties shall:

22.4.2.1. Make sure that the Services provided before the date of termination of the Contract and other actions performed meet the requirements of the Contract, and the Parties no longer make any claims against each other;
22.4.2.2. Pay for the Services provided before the termination of the Contract that meet the requirements thereof;
22.4.2.3. Within 10 (ten) days from the date of receipt of the notice of termination of the Contract or the date of conclusion of the Arrangement on termination of the Contract, to transfer to each other all the documents to be transferred in accordance with the provisions of the Contract.

23. CHANGE OF THE PRODUCT MODEL OR A MANUFACTURER

23.1. In cases when products are procured together with the Services, the Provider shall have the right to change the model of products and/or the manufacturer if all the following conditions are met:
23.1.1. If the products specified in the tender bid are no longer produced, or their delivery has been substantially disrupted and manufacturer's confirmation has been received, and/or the products, their manufacturer poses a threat to national security and/or supply of the products is in conflict with the mandatory international sanctions implemented in the Republic of Lithuania as defined in the Law on International Sanctions, and/or the products, their components or/and the manufacturer does not comply with the provisions of Article 45(2^1) of the Law on Public Procurement;
23.1.2. If the products substituted fully comply with all the requirements of the Procurement documents; they are at least of the same or better quality than the products described in the tender bid, and the Provider presents supporting documents; If the Provider has provided samples of the products during the Procurement procedures, the products to be delivered must be of at least the same quality as the samples provided;
23.1.3. If the Provider submitted a written request to the Buyer with the documents supporting the substitution and received the written consent thereof not later than 10 (ten) days before the intended substitution of the products. The Buyer shall have the right to object to the substitution of the products and terminate the Contract if the Provider has not provided evidence, or the evidence provided does not justify the compliance of the substituted products with the Procurement documents and prove the equivalent or better quality than that of the products specified in the Contract;
23.1.4. The Parties have concluded a written Arrangement to the Contract on the substitution of the products.
23.2. In case specified in this Section of the General Conditions, the products must be delivered at a price not higher than that indicated in the tender bid.

24.COMMUNICATION PROCEDURE AND LANGUAGE

24.1. The Contract shall be concluded in Lithuanian. If the Contract or any document forming an integral part thereof is concluded in another language or translated into another language, in all cases only the text of the Contract drawn up in Lithuanian shall be considered authentic (if there are discrepancies, the text in Lithuanian shall prevail).
24.2. If a Party notifies the other Party of its new contact details and the other Party receives such notification, it shall send all notifications and information to be sent under the Contract to the new contact details. If a Party does not notify of a change in contact details, or until the other Party does

not receive such a notification, sending of the notification to the last contact details known to the Party shall be deemed adequate and relevant.

24.3. If a notification is delivered in person or sent by post or courier, it must be served upon signed acknowledgement and considered received on the date indicated in the acknowledgement of receipt.

24.4. If a notification is sent by e-mail, it shall be deemed to have been received by the Party on the next working day.

24.5. If a notification is sent in several different ways, the recipient shall be deemed to have received it when it received the first notification.

25.CLAIMS AND DISPUTE RESOLUTION

25.1. Any disputes, disagreements or claims arising out of or in connection with the Contract, its breach, termination or validity must be settled by negotiation between, in particular, the managers of the Parties or persons authorised by them.

25.2. If the Parties do not settle the dispute by negotiation, such dispute, disagreement or claim arising out of or in connection with this Contract or its breach, termination or invalidity shall be finally settled in courts of the Republic of Lithuania in accordance with the procedure laid down in the laws of the Republic of Lithuania.

25.3. Disputes shall not give rise to any grounds for the Parties to refuse the discharge of their obligations under the Contract.

PASLAUGŲ VIEŠOJO PIRKIMO–PARDAVIMO SUTARTIES BENDROJI DALIS

1. SUTARTIES SĄVOKOS

Šioje Sutartyje didžiąja raide rašomos pagrindinės sąvokos turi žemiau nurodytas reikšmes:

1.1. Aktas – Tiekėjui suteikus Paslaugas, pristačius Prekes ar įvykdžius Darbus Šalių (įgaliotų asmenų, už sutarties tinkamą vykdymą atsakingo asmens) pasirašomas Paslaugų, Prekių ar (ir) Darbų perdavimo – priėmimo aktas ar kitas lygiavertis dokumentas, patvirtintas Šalių parašais.

1.2. CVP IS – Centrinė viešųjų pirkimų informacinė sistema, leidžianti Užsakovui elektroniniu būdu organizuoti, o tiekėjams – dalyvauti viešuosiuose pirkimuose.

1.3. Užsakovas – Sutarties SD nurodytas juridinis asmuo, perkantis Sutarties SD nurodytą Sutarties objektą.

1.4. Tiekėjas – asmuo ar asmenų grupė, nurodytas šios Sutarties SD, teikiantis Sutartyje nurodytas Paslaugas Užsakovui.

1.5. Šalis – Užsakovas arba Tiekėjas, kiekvienas atskirai. Šalys – Užsakovas ir Tiekėjas abu kartu.

1.6. Trečioji šalis – bet kuris kitas fizinis arba juridinis asmuo, kuris nėra šios Sutarties Šalis.

1.7. Ūkio subjektas – juridinis arba fizinis asmuo, kurio pajėgumais remiasi Tiekėjas, kad atitiktų Pirkimo sąlygose nustatytus kvalifikacijos reikalavimus. Tuo atveju, Jei Tiekėjas tik remiasi kito ūkio subjekto ištekliais, toliau Sutartyje tokie ūkio subjektai vadinami Trečiaisiais asmenimis.

1.8. Įstatymas – Lietuvos Respublikos viešųjų pirkimų įstatymas.

1.9. Sutarties kaina – Sutarties SD nurodyta pagal Sutartį Tiekėjui mokėtina bendra suma, nurodyta Sutarties SD 6.4. p.

1.10. Pradinė sutarties vertė – Sutarties SD nurodyta bendra Sutarties kaina (be PVM), neatsižvelgiant į Sutarties pakeitimus po jos sudarymo.

1.11. Paslaugos – Sutarties SD nurodytos Paslaugos, teikiamos Sutartyje nustatyta tvarka ir terminais.

1.12. Pasiūlymas – Perkančiajai organizacijai vykdant Pirkimo procedūras, Tiekėjo pateiktų dokumentų visuma.

1.13. Pirkimo sąlygos – Užsakovo vykdytų Pirkimo procedūrų metu tiekėjams pateiktų Pirkimo dokumentų visuma, kuriais vadovaujantis Tiekėjas pateikė Pasiūlymą.

1.14. Sutartis – ši sutartis, kurią sudaro Sutarties SD, Sutarties BD ir Sutarties SD išvardyti priedai ir Susitarimai.

1.15. Sutarties Bendroji dalis (toliau – Sutarties BD) – šis dokumentas, kuris yra sudėtinė ir neatskiriama Sutarties dalis, nustatanti standartines Sutarties nuostatas bei standartines Užsakovo ir Tiekėjo teises, pareigas bei atsakomybę.

1.16. Sutarties Specialioji dalis (toliau – Sutarties SD) – Sutarties specialioji dalis, kurioje detalizuojamas Sutarties objektas, Paslaugų apimtis, kaina bei įkainiai (jei taikomi), kainos / įkainių peržiūros procedūra, Paslaugų teikimo terminai bei kitos Šalių sutartos sąlygos.

1.17. Sutarties įvykdymo užtikrinimas – Lietuvos Respublikoje ar užsienio valstybėje registruoto banko ar kitos kredito įstaigos išduota Sutarties sąlygų įvykdymo užtikrinimo garantija, draudimo bendrovės išduotas laidavimo draudimo raštas, arba Tiekėjo išduota garantija deponuojant lėšas Užsakovo banko sąskaitoje.

1.18. Techninė specifikacija – dokumentas, kuriame nurodytas Pirkimo objekto aprašymas, techniniai, kokybės ir kiti reikalavimai.

1.19. Teisės aktai – Lietuvos Respublikos Konstitucijoje, Lietuvos Respublikos teisėkūros pagrindų įstatyme ir kituose Lietuvos Respublikos įstatymuose įtvirtinta tvarka ir forma priimtas teisės aktas, kuriame nustatomos, keičiamos ar naikinamos teisės normos, skirtos neapibrėžtai subjektų ar atvejų grupei.

1.20. Užsakymas – Tiekėjui raštu teikiamas užsakymas dėl Paslaugų teikimo. Užsakymas laikomas gautu jo išsiuntimo dieną arba po 5 (penkių) dienų, jei siunčiamas Šalies registruotu paštu arba laikomas gautu įteikimo momentu, jei įteikiamas tiesiogiai.

1.21. Specialistas – Sutartyje numatytų Paslaugų teikimui Tiekėjo pasitelkiamas specialistas (darbuotojas), kurio profesine kvalifikacija ir (arba) patirtimi rėmėsi Tiekėjas tam, kad atitiktų Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus (jei taikoma), ir (arba) į kurio kvalifikaciją atsižvelgė Užsakovas, vertindamas Tiekėjo pasiūlymą (jei taikoma).

2. SUTARTIES OBJEKTAS

2.1. Šios Sutarties objektas yra nurodytas Sutarties SD.

2.2. Sutarties pagrindu gali būti teikiamos Paslaugos ar su Paslaugomis susijusios Prekės ir (ar) atliekami Darbai, kuriems *mutatis mutandis* taikomos Sutarties nuostatos ir Teisės aktų reikalavimai pagal Prekių / Darbų pobūdį bei Techninės specifikacijos reikalavimus.

3. SUTARTIES ĮSIGALIOJIMAS, ĮVYKDYMO UŽTIKRINIMAS, STRUKTŪRA IR AIŠKINIMAS

3.1. Sutarties įsigaliojimas yra nurodytas Sutarties SD.

3.2. Sutarties įvykdymo užtikrinimo taikymas yra nurodytas Sutarties SD (jei taikoma).

3.2.1. Sutarties įvykdymo užtikrinimas yra skirtas visų Tiekėjo sutartinių įsipareigojimų įvykdymo užtikrinimui, įskaitant, bet neapsiribojant, netesybų mokėjimui užtikrinti. Jei Sutartis yra nutraukiama dėl bet kokios priežasties, Sutarties įvykdymo užtikrinimas gali būti panaudotas bet kokiai iš Tiekėjo Užsakovui priklausančiai pinigų sumai susigrąžinti. Sutarties įvykdymo užtikrinimu Užsakovas gali pasinaudoti, nepriklausomai nuo Sutarties nutraukimo.

3.2.2. Pratęsus Tiekėjo sutartinių įsipareigojimų įvykdymo terminą, sustabdžius Sutarties vykdymą, ar Tiekėjui vėluojant įvykdyti Sutartinius įsipareigojimus, atitinkamai turi būti pratęstas ir Sutarties įvykdymo užtikrinimo galiojimo terminas. Tiekėjas turi užtikrinti, kad pratęsiant Sutarties įvykdymo užtikrinimo terminą neatsirastų laikotarpis, per kurį Tiekėjo prievolių vykdymas būtų neužtikrintas.

3.2.3. Sutarties įvykdymo užtikrinimas ir (ar) užtikrinimą patvirtinantis dokumentas per 5 darbo dienas nuo Tiekėjo rašytinio pareikalavimo pateikimo momento grąžinamas Tiekėjui, jei jis laiku ir tinkamai įvykdė visus sutartinius įsipareigojimus arba Sutarties įvykdymo užtikrinimas tapo nebereikalingas.

3.2.4. Jeigu Sutarties galiojimo metu, baigiasi Sutarties sąlygų vykdymo užtikrinimas, Tiekėjas ne vėliau, kaip likus 10 darbo dienų iki Sutarties sąlygų įvykdymo užtikrinimo pabaigos, turi pateikti Užsakovui naują Sutarties sąlygų įvykdymo užtikrinimo dokumentą, kuris galiotų iki Sutarties galiojimo pabaigos.

3.2.5. Tiekėjas įsipareigoja Užsakovui pasinaudojus sutarties įvykdymo užtikrinimu, per 10 darbo dienų pateikti naują Sutarties sąlygų įvykdymo užtikrinimo dokumentą.

3.3. Ši Sutartis yra vientisas ir nedalomas dokumentas, kurį sudaro visi toliau išvardinti dokumentai. Sutarties aiškinimo ir taikymo tikslais nustatoma tokia Sutarties dokumentų viršenybės tvarka:

3.3.1. Skelbimas apie pirkimą;

3.3.2. Sutarties SD;

3.3.3. Sutarties SD priedas „Techninė specifikacija“;

3.3.4. Sutarties BD;

3.3.5. Pirkimo sąlygos;

3.3.6. Pirkimo sąlygų priedai;

3.3.7. Tiekėjo pasiūlymas.

3.4. Jei Sutarties dokumentuose yra neaiškumų, neatitikimų ar prieštaravimų, taisyklės, nustatytos aukštesnės galios Sutarties dokumente, visuomet yra laikomos pakeičiančiomis žemesnės galios Sutarties dokumente nustatytas analogiškas taisykles nuo Sutarties įsigaliojimo dienos. Tuo atveju, jei Sutarties dalimi laikomi Paslaugų teikėjo pateikti dokumentai, įskaitant licencijas, jų naudojimo taisyklės ar pan., tai visos Paslaugų teikėjo pateiktų dokumentų nuostatos, prieštaraujančios Įstatymui ir (ar) Pirkimo sąlygoms, laikomos negaliojančiomis

3.5. Sutarčiai taikoma ir ji aiškinama pagal Lietuvos Respublikos teisę. Visoms teisėms ir įsipareigojimams pagal Sutartį yra taikomi Lietuvos Respublikos teisės aktai.

4. ŠALIŲ TEISĖS IR PAREIGOS

4.1. Užsakovas įsipareigoja:

4.1.1. per Sutarties SD nurodytą terminą, bet ne vėliau kaip iki Akto pasirašymo, patikrinti suteiktas Paslaugas bei įforminti patikrinimo rezultatus;

4.1.2. priimti Sutartyje nustatytais terminais ir tvarka Tiekėjo suteiktas Paslaugas, atitinkančias Techninės specifikacijos nustatytus reikalavimus;

4.1.3. sumokėti Tiekėjui už priimtas Paslaugas Sutartyje nustatytą kainą Sutartyje nustatytomis sąlygomis ir tvarka;

4.1.4. bendradarbiauti su Tiekėju: suteikti Tiekėjui jo pagrįstai prašomą, Užsakovo turimą informaciją ir (ar) dokumentus, būtinus Sutarčiai tinkamai ir laiku įvykdyti;

4.2. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose.

4.3. Kiti Užsakovo įsipareigojimai nurodyti Sutarties SD.

4.4. **Užsakovas turi teisę:**

4.4.1. reikalauti, kad Tiekėjas tinkamai ir laiku vykdytų įsipareigojimus, nurodytus Sutartyje bei Lietuvos Respublikoje galiojančiuose teisės aktuose;

4.4.2. tikrinti Paslaugų teikimo procesą tiek, kiek tai susiję su teikiamų Paslaugų kokybe, pareikšti Tiekėjui pastabas ir pasiūlymus dėl Paslaugų teikimo. Užsakovo pastebėti trūkumai fiksuojami raštu arba el. paštu ir turi būti Tiekėjo sąskaita ištaisyti per Užsakovo nurodytą terminą;

4.4.3. neapmokėti Europos elektroninių sąskaitų faktūrų standarto neatitinkančių sąskaitų, jeigu Tiekėjas jas pateikia ne Sutarties 5.10 punkte numatytomis priemonėmis;

4.4.4. išskaičiuoti netesybas ir kitus dėl Tiekėjo kaltės patirtus nuostolius iš Tiekėjui mokėtinų sumų, apie tai raštu informavęs Tiekėją;

4.4.5. sustabdyti mokėjimus Tiekėjui, jeigu Tiekėjas nevykdo arba netinkamai vykdo bet kokius Sutartimi prisiimtus ar teisės aktuose numatytus įsipareigojimus, iki kol šie įsipareigojimai nebus tinkamai įvykdyti;

4.4.6. bet kuriuo pirkimo sutarties galiojimo metu pareikalauti Tiekėjo pateikti pagrindžiančius dokumentus dėl Įstatymo 37 straipsnio 9 dalyje, 45 straipsnio 2^{1} dalyje ir (ar) 47 straipsnio 9 dalyje nurodytų aplinkybių buvimo / nebuvimo. Tiekėjui per perkančiosios organizacijos nustatytą terminą nepateiktus tokios informacijos, perkančioji organizacija turi teisę nesikreipdama į teismą, vienašališkai nutraukti pirkimo sutartį, raštu įspėjusi tiekėją prieš 10 kalendorinių dienų;

4.4.7. prašyti, kad Tiekėjas pateiktų visus dokumentus, numatytus Techninėje specifikacijoje ir Sutartyje.

4.5. Užsakovas turi kitas teises, numatytas Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose.

4.6. Kitos Užsakovo teisės nurodytos Sutarties SD.

4.7. **Tiekėjas įsipareigoja:**

4.7.1. nedelsiant, bet ne vėliau nei per Sutarties SD nurodytą terminą raštu informuoti Užsakovą apie bet kokias aplinkybes, trukdančias ir (ar) galinčias sutrukdyti Tiekėjui įvykdyti sutartinius įsipareigojimus Sutartyje nustatytais terminais bei tvarka. Toks pranešimas nepanaikina Užsakovo teisės

skaičiuoti netesybas pagal Sutartį ar reikalauti atlyginti kitus nuostolius, jeigu Paslaugos nebūtų suteiktos laiku;

4.7.2. tinkamai ir kokybiškai suteikti Paslaugas, atitinkančias Techninės specifikacijos nustatytus reikalavimus, Sutartyje nustatytais terminais ir tvarka;

4.7.3. Paslaugas teikti savo rizika bei sąskaita kaip įmanoma rūpestingai bei efektyviai, įskaitant, bet neapsiribojant, pagal geriausius visuotinai pripažįstamus profesinius, techninius standartus ir praktiką, panaudodamas visus turimus ar reikiamus įgūdžius, žinias ir išteklius;

4.7.4. Užsakovo reikalavimu, per Užsakovo nurodytą terminą pateikti Užsakovui visą informaciją ar dokumentus ir (ar) ataskaitą apie Sutarties vykdymo eigą;

4.7.5. užtikrinti, kad Sutarties sudarymo metu ir visą jos galiojimo laikotarpį Sutartį vykdytų Tiekėjo ir (ar) jo pasitelkto ūkio subjekto (-ų) (jeigu pasitelkiamas) darbuotojai, turintys Sutarties vykdymui reikalingą kvalifikaciją ir patirtį, atitinkančią Pirkimo dokumentuose bei galiojančiuose teisės aktuose nustatytus reikalavimus. Taip pat užtikrinti, kad visą Sutarties galiojimo laikotarpį Tiekėjo ir jo pasitelkto subtiekėjo (-ų) kvalifikacija atitiks pirkimo dokumentų ir teisės aktų nustatytus reikalavimus;

4.7.6. Užsakovui raštu paprašius, ne vėliau kaip per 3 darbo dienas nuo prašymo gavimo dienos arba Užsakovo nurodytu terminu grąžinti visus iš Užsakovo gautus Sutarčiai vykdyti reikalingus dokumentus;

4.7.7. užtikrinti iš Užsakovo Sutarties vykdymo metu gautos ir su Sutarties vykdymu susijusios informacijos konfidencialumą ir apsaugą;

4.7.8. Tiekėjo darbuotojai, kuriems dėl priskirtų funkcijų ar pavesto darbo būtų suteikta teisė be palydos patekti prie Užsakovo valdomų nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto ar priimti sprendimus dėl šių įrenginių ir turto funkcionavimo, turi atitikti Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 17 straipsnio 2 dalyje nustatytus kriterijus.

4.7.9. Pirkimo sutarties vykdymo metu užtikrinti atitiktį Įstatymo 37 straipsnio 9 dalyje, 45 straipsnio 2^1 dalyje ir 47 straipsnio 9 dalyje nustatytiems reikalavimams;

4.8. laikytis šių aplinkosaugos reikalavimų: mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, rengiama dokumentacija, paslaugų perdavimo–priėmimo aktai Užsakovui turi būti pateikti tik elektroniniu formatu, o dokumentacija, kuri turi būti pasirašoma ir paslaugų perdavimo–priėmimo aktai turi būti pasirašomi elektroniniu parašu. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka minimalius aplinkos apsaugos kriterijus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakyme Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ (aktuali redakcija);

4.9. Jei yra galimybė Paslaugas teikti nuotoliniu būdu;

4.10. Tiekėjas įsipareigoja tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose;

4.11. Kiti Tiekėjo įsipareigojimai nurodyti Sutarties SD.

4.12. **Tiekėjas turi teisę:**

4.12.1. reikalauti, kad Užsakovas priimtų kokybiškai ir laiku suteiktas Paslaugas, atitinkančias Sutarties ir Techninės specifikacijos, taip pat Paslaugų teikimui taikomų teisės aktų nustatytus reikalavimus, bei sumokėtų už jas Sutartyje nustatytą kainą Sutartyje nustatytomis sąlygomis ir tvarka;

4.12.2. reikalauti, kad Užsakovas tinkamai ir laiku vykdytų kitus įsipareigojimus, nurodytus Sutartyje ir Lietuvos Respublikoje galiojančiuose teisės aktuose;

4.12.3. prašyti, kad Užsakovas pateiktų turimus dokumentus ir (ar) kitą informaciją, kurie yra būtini Tiekėjui tinkamam Sutartimi prisiimtų įsipareigojimu įvykdymui;

4.12.4. Kitos Tiekėjo teisės nurodytos Sutarties SD.

5. SUTARTIES KAINA IR MOKĖJIMO TVARKA

5.1. Sutarčiai taikoma kainodara (vadovaujantis Kainodaros taisyklių nustatymo metodika, patvirtinta Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 28 d. įsakymu Nr. 1S-95 „Dėl kainodaros taisyklių nustatymo metodikos patvirtinimo“) nurodyta Sutarties SD.

5.2. Pradinė Sutarties vertė nurodyta Sutarties SD.

5.3. Sutarties kaina nurodyta Sutarties SD.

5.4. Paslaugų kainos / įkainių perskaičiavimo tvarka nurodyta Sutarties SD.

5.5. Atsiskaitymo tvarka nurodyta Sutarties SD.

5.6. Avanso mokėjimo galimybė nurodyta Sutarties SD (jei taikoma).

5.6.1. Avanso mokėjimo tvarka, kai už Paslaugas atsikaitoma etapais:

5.6.1.1. Tiekėjui išmokėtas avansas užskaitomas kaip dalinis apmokėjimas už suteiktas Paslaugas. Likusi Sutarties kaina už suteiktas Paslaugas sumokama dalimis pasirašius Aktus ir Tiekėjui Sutartyje nustatyta tvarka pateikus sąskaitas faktūras.

5.6.1.2. Kai Tiekėjui buvo išmokėtas avansas ir Tiekėjas vėluoja suteikti Paslaugas, jis, papildomai prie pagal Sutarties SD 9.2 papunktį mokėtinų sumų, turi mokėti 10 proc. dydžio metines palūkanas už vėlavimo laiką nuo jam išmokėtos avanso sumos, bet ne ilgiau kaip už 1 mėnesį.

5.6.1.3. Nutraukus Sutartį Tiekėjas privalo grąžinti Užsakovui gautą avansą per 7 darbo dienas (jeigu dalis Paslaugų suteikta, Užsakovas jas yra priėmęs – grąžinama neužskaityta avanso dalis, Užsakovas pasinaudoja avanso užtikrinimu (jei taikoma). Tais atvejais, jei nebuvo taikytas Sutarties SD 4.1 papunktis, Tiekėjas turi sumokėti 10 proc. procentų dydžio metines palūkanas nuo grąžintinos avanso sumos už laikotarpį nuo avanso išmokėjimo iki jo grąžinimo.

5.6.2. Avanso mokėjimo tvarka, kai už Paslaugas atsiskaitoma vienu mokėjimu:

5.6.2.1. Kai išmokėtas avansas, likusi Sutarties kaina sumokama suteikus visas Paslaugas. Kai avansas neišmokėtas (Tiekėjui nepaprašius ar nepateikus tinkamo išankstinio mokėjimo grąžinimo užtikrinimo), visa Sutarties kaina už suteiktas Paslaugas sumokama pasirašius Aktą ir Tiekėjui Sutartyje nustatyta tvarka pateikus sąskaitą faktūrą.

5.6.2.2. Nutraukus Sutartį Tiekėjas privalo grąžinti Užsakovui gautą avansą per 7 darbo dienas (jeigu dalis Paslaugų suteikta, Užsakovas jas yra priėmęs – grąžinama ta avanso dalis, kuri viršija Užsakovo priimtų Paslaugų kainą). Jei Tiekėjas negrąžina gauto avanso, Užsakovas pasinaudoja avanso užtikrinimu (jei taikoma). Tais atvejais, jei buvo taikytas Sutarties SD 6.7**Klaida! Nerastas nuorodos šaltinis.** punktas, Tiekėjas turi sumokėti 10 procentų dydžio metines palūkanas nuo grąžintinos avanso sumos už laikotarpį nuo avanso išmokėjimo iki jo grąžinimo.

5.7. Į Paslaugų kainą / įkainius yra įskaičiuoti visi mokesčiai ir visos Tiekėjo išlaidos, apimančios viską, ko reikia visiškam ir tinkamam Sutarties įvykdymui (įskaitant sąskaitų faktūrų pateikimo Sutarties BD 5.10. punkte numatytomis priemonėmis išlaidas).

5.8. Jeigu Sutarties vykdymo metu pasikeičia PVM mokėjimą reglamentuojantys teisės aktai, darantys tiesioginę įtaką Tiekėjo tiekiamų Paslaugų Sutartyje nurodytai kainai / įkainiams, Sutartyje nurodyta Paslaugų kaina / įkainiai perskaičiuojami ją / juos didinant arba mažinant. Perskaičiavimas įforminamas Sutarties pakeitimu, kuris tampa neatskiriama Sutarties dalimi. Perskaičiuota kaina / įkainiai taikomi už tą Paslaugų dalį, už kurią sąskaita faktūra išrašoma galiojant naujam PVM. Jeigu Paslaugų kainos / įkainių perskaičiavimą dėl pasikeitusio (padidėjusio ar sumažėjusio) PVM inicijuoja Tiekėjas, jis turi raštu kreiptis į Užsakovą ir pateikti konkrečius skaičiavimus dėl pasikeitusio PVM įtakos Paslaugų kainai / įkainiams. Užsakovas taip pat turi teisę inicijuoti kainos/įkainių perskaičiavimą dėl pasikeitusio PVM.

5.9. Jei Sutarties kaina buvo peržiūrėta pagal Sutartyje nurodytas kainų peržiūros sąlygas, atitinkamai patikslinama (didėja arba mažėja) Pradinė sutarties vertė.

5.10. Vykdant Sutartį, sąskaitos faktūros teikiamos tik elektroniniu būdu, per Sutarties SD 6.6. punkte nurodytą terminą. Elektroninės sąskaitos faktūros, atitinkančios Europos elektroninių sąskaitų faktūrų standartą, kurio nuoroda paskelbta 2017 m. spalio 16 d. Komisijos įgyvendinimo sprendime (ES) 2017/1870 dėl nuorodos į Europos elektroninių sąskaitų faktūrų standartą ir sintaksių sąrašo paskelbimo pagal Europos Parlamento ir Tarybos direktyvą 2014/55/ES (OL 2017 L 266, p. 19) (toliau – **Europos elektroninių sąskaitų faktūrų standartas**), teikiamos Tiekėjo pasirinktomis priemonėmis. Europos elektroninių sąskaitų faktūrų standarto neatitinkančios elektroninės sąskaitos faktūros gali būti teikiamos tik naudojantis sąskaitų administravimo bendrosios informacinės sistemos (SABIS) priemonėmis. Išankstinio mokėjimo sąskaitas (jeigu Sutarties SD 6.7. p. yra numatytas avanso mokėjimas) Tiekėjas privalo pateikti šiame Sutarties punkte nustatyta tvarka.

5.11. Sumokėjimo diena – tai diena, kai lėšos išskaitomos iš Užsakovo sąskaitos. Jeigu mokėjimo termino diena sutampa su poilsio diena, tai mokėjimų pagal Sutartį mokėjimo diena laikoma po jos einanti darbo diena.

6. PASLAUGŲ PERDAVIMO IR PRIĖMIMO TVARKA

6.1. Paslaugų teikimo rezultatas Užsakovui perduodamas Sutarties šalims pasirašant Paslaugų perdavimo–priėmimo aktą. Akto pasirašymo terminas nurodytas Sutarties SD.

6.2. Tiekėjas, įvykdęs Sutartyje numatytus įsipareigojimus, turi kreiptis į Užsakovą dėl Paslaugų rezultato Užsakovui perdavimo ir Paslaugų perdavimo–priėmimo akto pasirašymo. Užsakovas įsipareigoja priimti tinkamai ir laiku suteiktas Paslaugas, pasirašydamas Paslaugų perdavimo–priėmimo aktą.

6.3. Jeigu Paslaugų vykdymo ir (ar) Paslaugų perdavimo–priėmimo metu nustatoma, kad Paslaugos suteiktos netinkamai ir Paslaugų rezultatas neatitinka Sutartyje ir (ar) Techninėje specifikacijoje nustatytų reikalavimų, Užsakovas turi teisę atsisakyti pasirašyti Paslaugų perdavimo–priėmimo aktą, raštu Tiekėjui nurodydamas suteiktų Paslaugų trūkumus (jei įmanoma, nurodydamas ir priemones, kurių Tiekėjas privalo imtis, kad Paslaugų kokybė atitiktų Sutarties ir (ar) Techninės specifikacijos reikalavimus ir Paslaugų perdavimo–priėmimo aktas būtų pasirašytas). Jeigu Užsakovas atsisako pasirašyti Paslaugų perdavimo–priėmimo aktą ir praneša Tiekėjui, kad Paslaugos ar kuri nors Paslaugų dalis neatitinka Sutarties ir (ar) Techninės specifikacijos reikalavimų, Tiekėjas privalo savo sąskaita pašalinti nurodytus Sutarties vykdymo pažeidimus (neatitikimus) per Užsakovo nurodytą protingą terminą.

6.4. Tiekėjui nepašalinus Paslaugų trūkumų per Užsakovo nustatytą terminą, Užsakovas turi teisę vėliau perduodamų Paslaugų nepriimti ir už jas nesumokėti bei pateikti Tiekėjui pranešimą apie jų nepriėmimą.

6.5. Kartu su Paslaugų perdavimo–priėmimo aktu Tiekėjas turi pateikti Užsakovui visus dokumentus (dokumentai turi būti originalo kalba bei pateiktas patvirtintas vertimas į lietuvių kalbą, patvirtintas vertėjo parašu ir vertimų biuro antspaudu), kurie yra būtini teikiant Paslaugas sukurtų rezultatų naudojimui (jeigu taikoma).

7. PASLAUGŲ KOKYBĖ

7.1. Paslaugų garantinis terminas nustatomas Sutarties SD (jei taikoma) ir pradedamas skaičiuoti nuo Paslaugų ar jų dalies perdavimo Užsakovui, t. y. Akto pasirašymo dienos. Jei Garantinis terminas nenustatytas, tai neapriboja Užsakovo teisės Sutarties galiojimo metu pareikšti reikalavimus Tiekėjui dėl paslėptų Paslaugų trūkumų, kurių Užsakovas negalėjo nustatyti Paslaugų priėmimo metu. Trūkumai šalinami Tiekėjo sąskaita.

7.2. Vadovaujantis Lietuvos Respublikos civilinio kodekso (toliau – LR CK) 6.317 straipsniu, Tiekėjo garantija (patvirtinimas) dėl Prekių nuosavybės teisės ir jų kokybės yra, nepaisant to, ar tokia garantija Sutartyje numatyta, ar ne (garantija pagal įstatymą).

7.3. Tiekėjas, pasirašydamas Sutartį, garantuoja, kad teikiamos Paslaugos yra kokybiškos, atitinka visus Sutarties bei Teisės aktų reikalavimus, tinkamos naudoti pagal jų tikslinę paskirtį, be paslėptų trūkumų.

7.4. Paslaugų trūkumai pastebėti Paslaugų perdavimo – priėmimo metu ar (ir) po Akto pasirašymo turi būti pašalinti Sutarties SD nustatytais terminais Tiekėjo sąskaita. Apie pastebėtus Paslaugų trūkumus Užsakovas Tiekėjui turi praneši raštu. Užsakovas turi teisę nepriimti Paslaugų, jei Paslaugų perdavimo - priėmimo metu pastebimi Paslaugų trūkumai. Apie pastebėtus Paslaugų trūkumus yra pažymima Akte,

nurodant priimto sprendimo motyvus. Paslaugos gali būti Užsakovo priimamos su neesminiais trūkumais, Akte nurodant trūkumus ir terminą, per kurį trūkumai turi būti pašalinti (tik tais atvejais, jei Techninėje specifikacijoje nurodyta, kas bus laikoma neesminiais trūkumais). Visais atvejais visus Darbus ir (ar) Prekes, susijusius su Paslaugų trūkumų pašalinimu, Tiekėjas atlieka savo sąskaita per Sutarties SD nurodytą trūkumų šalinimo terminą (jei Šalys nesusitarė dėl trumpesnio termino). Sutartyje nustatytas atsiskaitymo terminas pradedamas skaičiuoti ir Užsakovui atsiranda prievolė atsiskaityti su Tiekėju tik po to, kai Užsakovas įsitikina, jog trūkumai, įskaitant neesminius, yra visiškai pašalinti. Trūkumų pašalinimas pažymimas Akte ir patvirtinamas Šalių parašais.

7.5. Tiekėjui per Sutarties SD nurodytą terminą nepašalinus Paslaugų perdavimo – priėmimo metu ir (ar) Garantinio termino galiojimo metu nustatytų trūkumų, Tiekėjas, Užsakovui pareikalavus, moka Sutarties SD nustatyto dydžio netesybas už vėlavimą pašalinti trūkumus bei atlygina Užsakovo dėl to patirtus nuostolius tiek, kiek jų nepadengia netesybos. Netesybų ir nuostolių sumokėjimas neatleidžia Tiekėjo nuo pareigos kuo skubiau pašalinti trūkumus.

7.6. Preziumuojama, kad Tiekėjas materialiai atsako už visus Paslaugų trūkumus, paaiškėjusius Paslaugų perdavimo – priėmimo metu ar (ir) Garantinio termino galiojimo metu, jeigu Tiekėjas neįrodo, kad Paslaugų trūkumai atsirado ne dėl Tiekėjo kaltės ar aplaidaus jo sutartinių įsipareigojimų vykdymo.

7.7. Prekių (ar jų dalies) / Darbų (ar jų dalies) Garantinis terminas nustatomas Sutartyje ir pradedamas skaičiuoti nuo Prekių ar jų dalies (jeigu Prekės tiekiamos dalimis) /Darbų ar jų dalies (jeigu Darbai atliekami dalimis), perdavimo Užsakovui dienos, t. y. Akto pasirašymo dienos (išskyrus jei Prekės / Darbai priimami su trūkumais, tokiu atveju terminas skaičiuojamas nuo įrašo Akte apie trūkumų pašalinimą dienos). Nustatytas Garantinis terminas neapriboja Užsakovo teisės pareikšti reikalavimus Tiekėjui dėl perduotų Prekių / Darbų trūkumų LR CK 6.338 straipsnyje nustatyta tvarka ir terminais.

8. ŠALIŲ ATSAKOMYBĖ

8.1. Tiekėjo ir Užsakovo civilinės atsakomybės sąlygos nurodytos Sutarties SD.

8.2. Užsakovas delspinigius Tiekėjui gali išskaičiuoti iš Tiekėjui pagal Sutartį mokėtinų sumų.

8.3. Šalys atsako už tai, kad Sutarties sąlygos būtų tinkamai vykdomos. Šalių atsakomybė yra nustatoma pagal galiojančius Lietuvos Respublikos teisės aktus ir Sutartį.

8.4. Tiekėjas privalo atlyginti Užsakovui dėl netinkamos kokybės suteiktų Paslaugų atsiradusią žalą.

8.5. Delspinigių sumokėjimas neatleidžia Sutarties šalių nuo pareigos vykdyti Sutartyje prisiimtus įsipareigojimus.

8.6. Tiekėjas visais atvejais atsako už Užsakovui paslaugų tiekimo metu jo pasitelktų asmenų padarytus nuostolius ar žalą, nepriklausomai nuo to, ar tokie nuostoliai ar žala būtų padaryta Užsakovui, jo darbuotojams ar bet kokiems tretiesiems asmenims ir jų turtui.

8.7. Tiekėjui netinkamai vykdant savo sutartinius įsipareigojimus Užsakovas turi teisę, neapribodamas kitų, Sutartyje ir teisės aktuose numatytų savo teisių gynimo priemonių taikymo galimybių, už įsipareigojimų nevykdymą taikyti vienašalį išskaitymą iš visų pagal Sutartį Tiekėjui mokėtinų sumų (pranešant apie tai Tiekėjui raštu), o, jei jų nepakaktų, ir iš Tiekėjo pateiktų prievolių įvykdymo užtikrinimų (jei taikoma), pranešant apie tai Tiekėjui raštu, Sutartyje nurodytoms netesyboms bei visiems Sutarties SD 9.4. p. nurodytiems nuostoliams padengti. Ši nuostata galioja nepaisant Sutarties nutraukimo bei kitų sankcijų taikymo.

9. NENUGALIMOS JĖGOS (FORCE MAJEURE) APLINKYBĖS

9.1. Šalis atleidžiama nuo atsakomybės už Sutarties neįvykdymą, jeigu ji įrodo, kad Sutartis neįvykdyta dėl aplinkybių, kurių ji negalėjo kontroliuoti bei protingai numatyti Sutarties sudarymo metu, ir kad negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui (*force majeure*).

9.2. Nenugalimos jėgos aplinkybėmis laikomos aplinkybės, nurodytos LR CK 6.212 straipsnyje ir Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklėse, patvirtintose Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo".

9.3. Šalis negalinti vykdyti pagal Sutartį savo įsipareigojimų dėl nenugalimos jėgos aplinkybių veikimo privalo raštu apie tai pranešti kitai šaliai per 10 dienų nuo tokių aplinkybių atsiradimo pradžios.

9.4. Nenugalimos jėgos aplinkybėms pasibaigus, toliau vykdomi Sutartyje numatyti šalių įsipareigojimai, jei šalys nesusitarta kitaip.

9.5. Jeigu nenugalimos jėgos aplinkybės ir jų padariniai tęsiasi ilgiau negu 3 mėnesius, kiekviena šalis turi teisę atsisakyti vykdyti savo įsipareigojimus ir nutraukti Sutartį.

10. SUTARTIES VYKDYMO SUSTABDYMAS

10.1. Sutarties vykdymo metu atsiradus nenumatytoms, nuo šalių nepriklausančioms aplinkybėms, atsiradusiomis ne dėl šalių valios (išskyrus nenugalimos jėgos (*force majeure*) aplinkybes), dėl kurių šalis negali vykdyti Sutarties ir kurių nebuvo galima numatyti Sutarties sudarymo metu (aplinkybės turi būti pagrįstos objektyviais faktais ir dokumentais iš kurių aiškiai būtų galima spręsti, kad tokios aplinkybės susiklostė), šalis nedelsiant pateikia tai patvirtinančius dokumentus kitai šaliai, kuri sprendžia klausimą dėl sutartinių įsipareigojimų ar jų dalies vykdymo sustabdymo iki minėtų aplinkybių išnykimo. Išnykus šiame punkte nurodytoms aplinkybėms, Sutarties vykdymas tęsiamas tam terminui, kiek buvo likę vykdyti Sutartį iki Sutarties vykdymo sustabdymo.

10.2. Jei sutartinių įsipareigojimų vykdymas dėl priežasčių, nepriklausančių nuo Tiekėjo buvo sustabdytas laikotarpiui, ne trumpesniam nei 90 dienų, praėjus 90 dienų Tiekėjas gali rašytiniu pranešimu Užsakovo pareikalauti atnaujinti sutartinių įsipareigojimų vykdymą per 14 dienų.

10.3. Užsakovas taip pat turi teisę sustabdyti sutartinių įsipareigojimų (ar jų dalies) vykdymą, jeigu jam pagrįstai kyla įtarimų dėl teikiamų Paslaugų kokybės ir reikia laiko patikrinti bei įsitikinti tiekiamų Paslaugų kokybe. Tokiu atveju sutartinių įsipareigojimų (ar jų dalies) vykdymo sustabdymas galimas iki 5 darbo dienų. Užsakovo galimybė pasinaudoti šia teise negali priklausyti nuo Tiekėjo valios ar būti jo įtakojama.

10.4. Išnykus aplinkybėms, lėmusioms sutartinių įsipareigojimų vykdymo sustabdymą, Sutarties vykdymas tęsiamas tam terminui, kiek buvo likę vykdyti Sutartį iki Sutarties vykdymo sustabdymo. Šalys norėdamos atnaujinti sustabdytų sutartinių įsipareigojimų (ar jų dalies) vykdymą turi viena kitą informuoti ne vėliau kaip prieš 3 darbo dienas.

10.5. Dėl sutartinių įsipareigojimų vykdymo sustabdymo visais atvejais turi būti sudaromas rašytinis susitarimas, nurodant motyvuotas priežastis ir sustabdymo terminą, bei pridedant dokumentus, patvirtinančius sustabdymo pagrindą (jeigu tokie yra).

11. SUTARTIES GALIOJIMAS, NUTRAUKIMAS IR KEITIMAS

11.1. Sutartis laikoma sudaryta, kai Šalys ranka, arba kvalifikuotu elektroniniu parašu, arba kitokiu Sutarties SD sutartu būdu pasirašo Sutarties SD ir Tiekėjas pateikia reikalaujamą Sutarties įvykdymo užtikrinimą (jeigu reikalaujama Sutarties SD). Jeigu Šalys šiuos dokumentus pasirašo ne vienu metu, Sutartis laikoma sudaryta tą dieną, kai Sutarties SD pasirašo paskutinioji Šalis. Tuo atveju, kai Tiekėjas pagal Sutarties SD turi pateikti Sutarties įvykdymo užtikrinimą (jeigu reikalaujama Sutarties SD) Sutartis įsigalioja kitą dieną po reikalaujamo Sutarties įvykdymo užtikrinimo.

11.2. Sutarties galiojimo terminas nurodytas Sutarties SD 3.2 p.

11.3. Tuo atveju, kai Tiekėjas pagal Sutarties SD turi pateikti Sutarties įvykdymo užtikrinimą (jeigu reikalaujama Sutarties SD) Sutartis įsigalioja kitą dieną po reikalaujamo Sutarties įvykdymo užtikrinimo Užsakovui pateikimo bei galioja iki visiško Sutarties šalių sutartinių įsipareigojimų įvykdymo arba Sutarties nutraukimo Sutartyje ar įstatymuose nustatytais atvejais.

11.4. Jeigu Tiekėjas nepateikia Užsakovui Sutarties įvykdymo užtikrinimo pagal Sutarties SD sąlygas, laikoma, kad Tiekėjas nepagrįstai atsisakė Sutarties. Tokiu atveju laikoma, kad kitą dieną po termino Tiekėjui pateikti Sutarties įvykdymo užtikrinimą Sutartis pasibaigia, Užsakovas įgyja teisę Įstatymų nustatyta tvarka pasiūlyti sudaryti Sutartį kitam tiekėjui ir reikalauti Tiekėjo atlyginti dėl to kylančius Užsakovo nuostolius bei tuo tikslu pasinaudoti Tiekėjo pasiūlymo galiojimo užtikrinimu, neviršydamas patirtų nuostolių sumos.

11.5. Jei kuri nors Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojančia, tai neturi įtakos kitų Sutarties nuostatų galiojimui.

11.6. Sutartis gali būti nutraukta:

11.6.1. rašytiniu abipusiu šalių susitarimu;

11.6.2. Sutartyje nustatytais atvejais ir tvarka;

11.6.3. kitais LR CK nustatytais atvejais.

11.7. Užsakovas, nesikreipdamas į teismą, gali vienašališkai nutraukti Sutartį, raštu įspėjęs Tiekėją prieš 10 (dešimt) kalendorinių dienų, jeigu:

11.7.1. Tiekėjui iškeliama restruktūrizavimo arba bankroto byla, Tiekėjas likviduojamas, sustabdo savo ūkinę veiklą arba kai įstatymuose ar kituose teisės aktuose nustatyta tvarka susidaro analogiška situacija, ir šios aplinkybės trukdo tinkamai laiku vykdyti Sutartimi prisiimtus įsipareigojimus;

11.7.2. esant esminiam Sutarties pažeidimui, kaip tai numatyta Sutartyje ir (ar) LR CK;

11.7.3. Sutartis buvo pakeista pažeidžiant Įstatymo 89 straipsnį;

11.7.4. paaiškėjo Įstatymo 37 straipsnio 9 dalyje, 45 straipsnio 2^1 dalyje ir (ar) 47 straipsnio 9 dalyje nurodytos aplinkybės;

11.7.5. paaiškėjo, kad Tiekėjas, su kuriuo sudaryta Sutartis, turėjo būti pašalintas iš Pirkimo procedūros pagal Įstatymo 46 straipsnio 1 dalį;

11.7.6. paaiškėjo, kad su Tiekėju neturėjo būti sudaryta Sutartis dėl to, kad Europos Sąjungos Teisingumo Teismas procese pagal Sutarties dėl Europos Sąjungos veikimo 258 straipsnį pripažino, kad nebuvo įvykdyti įsipareigojimai pagal Europos Sąjungos steigiamąsias sutartis ir Direktyvą 2014/24/ES;

11.7.7. Lietuvos Respublikos Vyriausybė Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo nustatyta tvarka priima sprendimą, patvirtinantį, kad Sutartis (jo pakeitimas) laikoma keliančia riziką ar neatitinka nacionalinio saugumo interesų;

11.7.8. jeigu Tiekėjas nepateikia naujo arba pratęsto Sutarties įvykdymo užtikrinimo Sutarties SD nurodyta tvarka, išskyrus pirminį sutarties užtikrinimą (jei reikalaujama Sutarties įvykdymo užtikrinimo);

11.7.9. jeigu Tiekėjas pažeidžia Sutartyje nustatytus įsipareigojimus dėl konfidencialumo;

11.7.10. Tiekėjas nepradeda laiku vykdyti Sutarties;

11.7.11. Sutarties vykdymo sustabdymas trunka ilgiau nei 90 dienų.

11.8. Užsakovas, be išankstinio įspėjimo gali nutraukti Sutartį vienašališkai dėl esminio sutarties pažeidimo ir reikalauti atlyginti nuostolius, jeigu:

11.8.1. Tiekėjas vėluoja pradėti teikti Paslaugas daugiau kaip Sutarties SD nurodyta terminą (jei taikoma);

11.8.2. delspinigių dydis pasiekia 20 proc. pradinės Sutarties vertės;

11.8.3. Tiekėjas, siekdamas sudaryti Sutartį su Užsakovu, buvo sudaręs susitarimą, neleistinai ribojantį konkurenciją;

11.8.4. Tiekėjas Sutarties vykdymo metu įtraukiamas į nepatikimų tiekėjų sąrašą arba subtiekėju pasitelkia asmenį, įtrauktą į nepatikimų tiekėjų sąrašą ir vadovaujantis VPĮ 46 str. 10 d. pateikia netinkamus „apsivalymo" dokumentus;

11.8.5. jeigu Tiekėjas be išankstinio raštiško Užsakovo sutikimo pakeitė jungtinės veiklos partnerį;

11.8.6. Tiekėjas (ar bent vienas iš Tiekėjo dalyvių, kai Tiekėjas yra ūkio subjektų grupė) prarado Įstatymo 23 straipsnyje nurodytą statusą arba tokį statusą prarado subtiekėjas ir Tiekėjas negali pakeisti tokio subtiekėjo kitu, reikalavimus atitinkančiu subtiekėju, o be subtiekėjo pats negali įvykdyti Sutarties.

11.9. Tiekėjas, nesikreipdamas į teismą, gali vienašališkai nutraukti Sutartį:

11.9.1. raštu įspėjęs Užsakovą apie Sutarties nutraukimą ne vėliau kaip prieš 20 (dvidešimt) kalendorinių dienų, jeigu Užsakovas ne dėl Tiekėjo kaltės arba nenugalimos jėgos aplinkybių vėluoja atlikti mokėjimą daugiau kaip 30 kalendorinių dienų ar padaro kitą esminį Sutarties pažeidimą, kaip tai numatyta LR CK;

11.9.2. Sutarties vykdymo sustabdymas trunka ilgiau nei 90 kalendorinių dienų.

11.10. Užsakovas nesant Tiekėjo kaltės, turi teisę vienašališkai nutraukti Sutartį įspėjęs apie tai Tiekėją ne vėliau kaip prieš 30 kalendorinių dienų, nepaisydamas to, kad Tiekėjas jau pradėjo ją vykdyti. Šiuo atveju Užsakovas privalo sumokėti Tiekėjui už iki Sutarties nutraukimo suteiktas Paslaugas.

11.11. Sutarties nutraukimas nepanaikina teisės reikalauti sumokėti netesybas, numatytas Sutartyje už sutartinių įsipareigojimų nevykdymą ar netinkamą vykdymą iki Sutarties nutraukimo, ir atlyginti nuostolius, patirtus dėl įsipareigojimų nevykdymo ar netinkamo vykdymo pagal šią Sutartį, kaip numatyta Sutarties nuostatose.

11.12. Kitais nei šiame skyriuje nustatytais atvejais Sutartis gali būti keičiama, tik jei tai galima, vadovaujantis Įstatymo 89 straipsnio nuostatomis.

11.13. Atsiradus poreikiui įsigyti papildomų paslaugų, Užsakovas kreipsis į Tiekėją su prašymu pateikti papildomų paslaugų kainas (jei papildomų paslaugų kainos viešai neskelbiamos), pažymėdamas, kad įsigytinų papildomų paslaugų kainos turi būti konkurencingos ir negali būti didesnės nei rinkos kainos. Gavęs Tiekėjo pateiktas papildomų paslaugų kainas (komercinį pasiūlymą), Užsakovas atlieka rinkos kainų tyrimą (apklausą telefonu ir / ar raštu, ir / ar paiešką elektroninėje erdvėje ar kt.), tokiu būdu įvertindamas, ar Teikėjo pateiktos papildomų paslaugų kainos atitinka rinką. Nustačius, kad Teikėjo pasiūlytos nenumatytų paslaugų kainos yra didesnės nei rinkos, Užsakovas prašo Teikėjo jas sumažinti. Tik objektyviai įvertinus ir turint pagrindžiančius / įrodančius dokumentus, kad Tiekėjo pateiktos papildomų paslaugų kainos atitinka rinkos kainas, jos gali būti įsigyjamos vadovaujantis šia Sutartimi.

11.14. Kitos Sutarties sąlygos Sutarties galiojimo laikotarpiu gali būti keičiamos Sutartyje ir Įstatyme nustatyta tvarka ir atvejais. Sutarties keitimas galioja tik tuo atveju, jeigu jis yra sudaromas rašytiniu Sutarties šalių susitarimu. Šalių susitarimai dėl Sutarties keitimo tampa neatskiriama Sutarties dalimi.

11.15. Vykdant sutartį, gali būti atliekami techninio pobūdžio sutarties pakeitimai. Techninio pobūdžio pakeitimais laikoma: sutarties šalių rekvizitai, kontaktinių asmenų pakeitimas, techninės klaidos. Techninio pobūdžio pakeitimai įforminami sutarties šalių atstovų pasirašytu susitarimu, kuris yra neatskiriama sutarties dalis.

12.SUBTIEKĖJAI IR JŲ KEITIMO TVARKA

12.1. Sutarties vykdymui Tiekėjas pasitelkia savo Pasiūlyme nurodytus subtiekėjus. Subtiekėjai nurodyti Sutarties SD.

12.2. Tiekėjas atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkiami subtiekėjai.

12.3. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Užsakovui pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Užsakovas taip pat reikalauja, kad Tiekėjas informuotų apie minėtos informacijos pasikeitimus visu Sutarties vykdymo metu, taip pat apie naujus subtiekėjus, kuriuos jis ketina pasitelkti vėliau.

12.4. Tiekėjas neturi teisės keisti subtiekėjų be Užsakovo raštiško sutikimo. **Subtiekėjų keitimo tvarkos pažeidimas bus laikomas esminiu Sutarties pažeidimu.**

12.5. Subtiekėjų keitimas ar naujų subtiekėjų pasitelkimas galimas tik tuomet, kai Tiekėjas Užsakovui pateikia pagrįstą prašymą dėl subtiekėjo, kuris nurodytas Sutartyje, keitimo ar naujo subtiekėjo pasitelkimo, naujo subtiekėjo atitiktį Pirkimo dokumentuose nustatytiems kvalifikaciniams reikalavimams pagrindžiančius dokumentus (jei Pirkimo dokumentuose subtiekėjams pagal prisiimtų sutartinių įsipareigojimų dalį buvo keliami kvalifikaciniai reikalavimai) ir subtiekėjo pašalinimo pagrindų nebuvimą patvirtinančius dokumentus (jei Pirkimo dokumentuose subtiekėjams buvo keliamas reikalavimas dėl pašalinimo pagrindų nebuvimo), bei gauna raštišką Užsakovo sutikimą dėl pasirinkto subtiekėjo pakeitimo ar naujo subtiekėjo pasitelkimo. Užsakovui sutikus su subtiekėjo pakeitimu ar naujo subtiekėjo pasitelkimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl subtiekėjo pakeitimo ar naujo subtiekėjo pasitelkimo, kurį pasirašo šalys. Šis susitarimas yra neatskiriama Sutarties dalis.

12.6. Jei Užsakovas turi pagrįstų įtarimų, kad subtiekėjas nekompetentingas vykdyti jam nustatytas pareigas, jis gali reikalauti, kad Tiekėjas pasitelktų kitą subtiekėją, kuris turėtų kvalifikaciją, atitinkančią Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus (jei Pirkimo dokumentuose subtiekėjams pagal prisiimtų sutartinių įsipareigojimų dalį buvo keliami kvalifikaciniai reikalavimai) ir nebūtų Pirkimo dokumentuose nustatytų šio subtiekėjo pašalinimo pagrindų (jei Pirkimo dokumentuose subtiekėjams buvo keliamas reikalavimas dėl pašalinimo pagrindų nebuvimo). Užsakovas raštišku prašymu kreipiasi į Tiekėją dėl šio subtiekėjo pakeitimo, nurodydamas motyvus. Tiekėjas, gavęs Užsakovo prašymą dėl Tiekėjo subtiekėjo pakeitimo, turi pareigą per protingą terminą, bet ne ilgesnį kaip 14 dienų, pasiūlyti kitą subtiekėją Sutarties vykdymui bei gauti Užsakovo sutikimą jo paskyrimui. Užsakovui sutikus su subtiekėjo pakeitimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl subtiekėjo pakeitimo, kurį pasirašo šalys. Šis susitarimas yra neatskiriama Sutarties dalis.

12.7. Jei Tiekėjas ne dėl Užsakovo kaltės per vieną mėnesį nuo tos dienos, kai paaiškėja, kad subtiekėjas nekompetentingas vykdyti nustatytas pareigas, į jo vietą nepaskiria kito Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus atitinkančio (jei Pirkimo dokumentuose subtiekėjams pagal prisiimtų sutartinių įsipareigojimų dalį buvo keliami kvalifikaciniai reikalavimai) subtiekėjo**, tai bus laikoma**

esminiu Sutarties pažeidimu, ir Užsakovas turi teisę vienašališkai nutraukti Sutartį ir taikyti kitas Sutartyje numatytas savo teisių gynimo priemones.

12.8. Subtiekėjams pageidaujant, Užsakovas su jais atsiskaitys tiesiogiai. Apie šią galimybę Užsakovas subtiekėją (-us) informuos atskiru pranešimu per 3 darbo dienas nuo informacijos iš Tiekėjo apie pasitelkiamą subtiekėją gavimo dienos. Norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, subtiekėjas turi apie tai raštu ne vėliau kaip per 5 darbo dienas informuoti Užsakovą. Tokiu atveju su Užsakovu, Tiekėju ir subtiekėju bus sudaroma trišalė sutartis, kurioje pateikiama tiesioginio atsiskaitymo su subtiekėju tvarka, įskaitant teisę Tiekėjui prieštarauti nepagrįstiems mokėjimams. Trišalės sutarties dėl tiesioginio atsiskaitymo su subtiekėju pasirašymas nekeičia Tiekėjo atsakomybės dėl Sutarties įvykdymo.

13.ŪKIO SUBJEKTAI, KURIŲ PAJĖGUMAIS REMIASI TIEKĖJAS IR JŲ KEITIMO TVARKA

13.1. Sutarties vykdymui Tiekėjas pasitelkia savo Pasiūlyme nurodytus ūkio subjektus. Ūkio subjektai nurodyti Sutarties SD.

13.2. Tiekėjas atsako už visus pagal Sutartį prisiimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkiami ūkio subjektai.

13.3. Tiekėjas neturi teisės keisti Sutarties SD nurodytų ūkio subjektų be Užsakovo raštiško sutikimo. **Ūkio subjektų keitimo tvarkos pažeidimas bus laikomas esminiu Sutarties pažeidimu.**

13.4. Ūkio subjektų keitimas ar naujų ūkio subjektų pasitelkimas galimas tik tuomet, kai Tiekėjas Užsakovui pateikia pagrįstą prašymą dėl ūkio subjekto, kuris nurodytas Sutartyje, keitimo ar naujo ūkio subjekto pasitelkimo, naujo ūkio subjekto atitiktį Pirkimo dokumentuose nustatytiems kvalifikaciniams reikalavimams pagrindžiančius dokumentus ir ūkio subjekto pašalinimo pagrindų nebuvimą patvirtinančius dokumentus, bei gauna raštišką Užsakovo sutikimą dėl pasirinkto ūkio subjekto pakeitimo ar naujo ūkio subjekto pasitelkimo. Užsakovui sutikus su ūkio subjekto pakeitimu ar naujo ūkio subjekto pasitelkimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl ūkio subjekto pakeitimo ar naujo ūkio subjekto pasitelkimo, kurį pasirašo šalys. Šis susitarimas yra neatskiriama Sutarties dalis.

13.5. Jei Užsakovas turi pagrįstų įtarimų, kad ūkio subjektas nekompetentingas vykdyti nustatytas pareigas, jis gali reikalauti, kad Tiekėjas pasitelktų kitą ūkio subjektą, kuris turėtų kvalifikaciją, atitinkančią Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus ir nebūtų Pirkimo dokumentuose nustatytų šio ūkio subjekto pašalinimo pagrindų. Užsakovas raštišku prašymu kreipiasi į Tiekėją dėl šio ūkio subjekto pakeitimo, nurodydamas motyvus. Tiekėjas, gavęs Užsakovo prašymą dėl ūkio subjekto pakeitimo, turi pareigą per protingą terminą, bet ne ilgesnį kaip 14 dienų, pasiūlyti kitą ūkio subjektą Sutarties vykdymui bei gauti Užsakovo sutikimą jo paskyrimui. Užsakovui sutikus su ūkio subjekto pakeitimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl ūkio subjekto pakeitimo, kurį pasirašo šalys. Šis susitarimas yra neatskiriama Sutarties dalis.

13.6. Tuo atveju, jei keičiamas ūkio subjektas už kurį Užsakovas vertindamas Pasiūlymą suteikė papildomus ekonominio naudingumo balus, Tiekėjas gali siūlyti tik tokį ūkio subjektą, kurio kvalifikacija būtų ne prastesnė nei ūkio subjekto, kuris keičiamas.

13.7. Jei Tiekėjas ne dėl Užsakovo kaltės per vieną mėnesį nuo tos dienos, kai paaiškėja, kad ūkio subjektas nekompetentingas vykdyti nustatytas pareigas, į jo vietą nepaskiria kito Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus atitinkančio ūkio subjekto**, tai bus laikoma esminiu Sutarties pažeidimu**, ir Užsakovas turi teisę vienašališkai nutraukti Sutartį ir taikyti kitas Sutartyje numatytas savo teisių gynimo priemones.

13.8. Tiekėjo pasitelkiamiems ūkio subjektams, kurie faktiškai vykdys sutartį, pageidaujant, Užsakovas su jais atsiskaitys tiesiogiai. Apie šią galimybę Užsakovas ūkio subjektą (-us) informuos atskiru pranešimu per 3 (tris) darbo dienas nuo informacijos iš Tiekėjo apie pasitelkiamą ūkio subjektą gavimo dienos. Norėdamas pasinaudoti tiesioginio atsiskaitymo galimybe, ūkio subjektas turi apie tai raštu ne vėliau kaip per 5 (penkias) darbo dienas informuoti Užsakovą. Tokiu atveju su Užsakovu, Tiekėju ir ūkio subjektu bus sudaroma trišalė sutartis, kurioje pateikiama tiesioginio atsiskaitymo su subtiekėju tvarka, įskaitant teisę Tiekėjui prieštarauti nepagrįstiems mokėjimams. Trišalės sutarties dėl tiesioginio atsiskaitymo su ūkio subjektu pasirašymas nekeičia Tiekėjo atsakomybės dėl Sutarties įvykdymo.

14.SUTARTIES VYKDYMUI PASKIRTI SPECIALISTAI IR JŲ KEITIMO TVARKA

14.1. Sutartį vykdys Tiekėjo Pasiūlyme nurodyti Specialistai. Specialistai nurodyti Sutarties SD.

14.2. Tiekėjas neturi teisės keisti Sutarties SD 10.3 – 10.4 p. nurodytų Specialistų (darbuotojų) be Užsakovo raštiško sutikimo. Sutartį vykdantys Tiekėjo Pasiūlyme nurodyti Specialistai (darbuotojai) gali būti keičiami tik dėl nuo Tiekėjo valios nepriklausančių aplinkybių (pvz. specialisto ligos, darbo santykių pabaigos ar esant kitoms svarbioms aplinkybėms). Sutarties SD 10.3 – 10.4 p. nurodytų Specialistų (darbuotojų) pakeitimas be Užsakovo raštiško sutikimo yra laikomas **esminiu Sutarties pažeidimu.**

14.3. Apie tai, kad Sutarties SD 10.3 – 10.4 p. nurodytas Specialistas (darbuotojas) (pvz. specialisto ligos, darbo santykių pabaigos ar esant kitoms svarbioms aplinkybėms) negali vykdyti Sutarties, Tiekėjas ne vėliau, kaip per 3 darbo dienas privalo informuoti Užsakovą ir pasiūlyti Užsakovui svarstyti naujo Specialisto kandidatūrą kartu pateikdamas reikiamus kandidato kvalifikaciją pagrindžiančius dokumentus. Siūlomo Specialisto kvalifikacija turi atitikti Pirkimo dokumentuose nustatytus kvalifikacijos ir/ar kokybinio vertinimo reikalavimus. Tuo atveju, jeigu keičiamas Specialistas nurodytas Sutarties SD 10.4. p., jo kvalifikacija turi būti ne žemesnė nei keičiamo Specialisto. Užsakovui sutikus su Specialisto (darbuotojo) pakeitimu ar naujo Specialisto (darbuotojo) pasitelkimu, Užsakovas kartu su Tiekėju raštu sudaro susitarimą dėl šio Specialisto (darbuotojo) pakeitimo ar naujo Specialisto (darbuotojo) pasitelkimo, kurį pasirašo šalys. Šis susitarimas yra neatskiriama Sutarties dalis.

14.4. Užsakovas turi teisę inicijuoti Specialisto (darbuotojo), kuris nevykdo ar netinkamai vykdo Sutartį, pakeitimą, nurodydamas tokio prašymo motyvus. Tiekėjas, gavęs šiame Sutarties punkte nurodytą

Užsakovo prašymą dėl paskirto Specialisto (darbuotojo) pakeitimo, turi pareigą per protingą, bet ne ilgesnį kaip 14 (keturiolikos) kalendorinių dienų terminą, pasiūlyti Užsakovui svarstyti naujo specialisto kandidatūrą, kurio kvalifikacija atitinka Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus, kartu pateikdamas reikiamus kandidato kvalifikaciją pagrindžiančius dokumentus. Užsakovui sutikus su naujai siūlomu specialistu (darbuotoju), šalys raštu sudaro susitarimą dėl šio Specialisto (darbuotojo) pakeitimo. Šis susitarimas yra neatskiriama Sutarties dalis.

14.5. Tiekėjas turi teisę inicijuoti papildomo naujo Specialisto, kuris atitinka Pirkimo dokumentuose nustatytus reikalavimus, kartu pateikdamas pagrindžiančius dokumentus (jeigu taikoma), įtraukimą į Sutarties vykdymą, nurodydamas tokio prašymo motyvus. Užsakovui sutikus su naujai siūlomo Specialisto (darbuotojo) įtraukimu, šalys raštu sudaro susitarimą dėl šio Specialisto (darbuotojo) įtraukimo. Šis susitarimas yra neatskiriama Sutarties dalis. Tiekėjo papildomai įtraukiamų specialistų skaičius nėra ribojamas.

14.6. Tuo atveju, jei keičiamas specialistas už kurį Užsakovas vertindamas Pasiūlymą suteikė papildomus ekonominio naudingumo balus, Tiekėjas gali siūlyti tik tokį specialistą, kurio kvalifikacija būtų ne prastesnė nei specialisto, kuris keičiamas.

14.7. Jei Tiekėjas ne dėl Užsakovo kaltės per vieną mėnesį nuo tos dienos, kai paaiškėja, kad specialistas (darbuotojas) negali vykdyti Sutarties, į jo vietą nepaskiria kito Pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus atitinkančio asmens, **tai bus laikoma esminiu Sutarties pažeidimu,** ir Užsakovas turi teisę vienašališkai nutraukti Sutartį ir taikyti kitas Sutartyje numatytas savo teisių gynimo priemones.

14.8. Užsakovas tvarkys šiuos Specialistų asmens duomenis: identifikacinius asmens duomenis (vardą, pavardę, telefono numerį, el. paštą ir asmens kodą (asmens kodas tvarkomas, kai Specialistui reikalinga prieiga prie Užsakovo duomenų bazės), kompiuterinės darbo vietos duomenis klientinio prisijungimo VPN technologijos atveju (kompiuterio vardą, serijinį numerį, IP adresą, MAC adresą, savininkystę, organizaciją, priskirto diegimo paketo serijinį numerį, ZTNA serijinį numerį, identifikacinį numerį ID, prisijungimo statusus).

15.SUSIRAŠINĖJIMAS

15.1. Visi pranešimai, sutikimai ir kitas susižinojimas, kuriuos šalis gali pateikti pagal šią Sutartį, teikiami lietuvių kalba. Visa informacija, įspėjimai ar pranešimai, susiję su šia Sutartimi, privalo būti raštiški ir turi būti siunčiami elektroniniu paštu, registruotu laišku ar kurjeriniu paštu (su patvirtinimu apie įteikimą) arba įteikiami pasirašytinai Sutarties rekvizituose nurodytais adresais kitai Sutarties šaliai. Pranešimai kitai Sutarties šaliai, išsiųsti elektroniniu paštu, yra laikomi gautais jų išsiuntimo dieną arba kitą darbo dieną, jeigu išsiuntimo diena buvo ne darbo diena. Pranešimai, siųsti registruotu laišku, laikomi įteiktais ne vėliau kaip per 3 (tris) darbo dienas nuo jų išsiuntimo dienos.

15.2. Jei pasikeičia šalies adresas ir (ar) kiti Sutartyje nurodyti duomenys, tokia šalis turi informuoti kitą šalį pranešdama ne vėliau, kaip per 3 kalendorines dienas nuo jų pasikeitimo momento. Jei šaliai nepavyksta laikytis šių reikalavimų, ji neturi teisės į pretenziją ar atsiliepimą, jei kitos šalies veiksmai, atlikti remiantis paskutiniais žinomais jai duomenimis, prieštarauja Sutarties sąlygoms arba ji negavo jokio pranešimo, išsiųsto pagal tuos duomenis.

16.ASMENS DUOMENŲ TVARKYMAS

16.1. Vykdydamos Sutartį šalys gautus asmens duomenis, nurodytus Sutartyje, kituose su Paslaugų viešuoju pirkimu susijusiuose dokumentuose tvarko kaip tų asmens duomenų valdytojos laikantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apaugos reglamentas) 5 straipsnyje nustatytų su asmens duomenų tvarkymu susijusių principų, tik esant bent vienai teisėto asmens duomenų tvarkymo sąlygai, nurodytai Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalyje ir užtikrindamos Bendrojo duomenų apsaugos reglamento, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą ir apsaugą, reikalavimų vykdymą.

16.2. Jei Tiekėjas, vykdydamas Sutartį, tvarko asmens duomenis Užsakovo vardu, kai Paslaugų teikimas yra susijęs su asmens duomenų tvarkymu, vadovaujantis Bendrojo duomenų apsaugos reglamento 4 straipsnio 8 punktu, 28 straipsnio 1 dalimi, Tiekėjas yra laikomas duomenų tvarkytoju. Tokiu atveju Tiekėjas ir Užsakovas, prieš pradedant Tiekėjui tvarkyti asmens duomenis, privalo pasirašyti asmens duomenų tvarkymo sutartį (susitarimą) dėl asmens duomenų tvarkymo, sudarytą vadovaujantis Bendrojo duomenų apsaugos reglamento 28 straipsnio 3 dalimi.

17.KONFIDENCIALUMAS

17.1. Tiekėjas įsipareigoja laikytis konfidencialumo įsipareigojimų, neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant Sutartį visu Sutarties galiojimo laikotarpiu ir jai pasibaigus 5 metus, išskyrus tiek, kiek tai reikalinga Sutarties vykdymui ir kai pagal įstatymus ar kitus norminius aktus yra numatytas ilgesnis konfidencialios informacijos saugojimo terminas, o taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams. Visa Tiekėjui atskleista informacija yra konfidenciali, išskyrus teisės aktuose numatytus atvejus bei Užsakovui raštu patvirtinus, kad tam tikra pateikta informacija nėra konfidenciali. Konfidencialia taip pat nėra laikoma informacija, kuri buvo viešai prieinama, arba Tiekėjas gali dokumentais įrodyti, kad informacija jam buvo teisėtai žinoma arba buvo pateikta trečiųjų asmenų, turėjusių raštu patvirtintą teisę atskleisti konfidencialią informaciją.

17.2. Konfidencialia informacija taip pat laikoma:

17.2.1. Bet kokiu būdu išreikšta informacija (rašytinė, žodinė, elektroninė ar vizualinė), kuria šalys apsikeičia Sutarties vykdymo metu;

17.2.2. Kita informacija, pažymėta kaip konfidenciali ar nors ir nepažymėta, bet pagal savo turinį ir pobūdį laikytina konfidencialia.

17.3. Kilus neaiškumui, ar informacija yra konfidenciali, Tiekėjas privalo kreiptis į Užsakovą dėl informacijos pobūdžio nustatymo.

17.4. Tiekėjas įsipareigoja:

17.4.1. kad Tiekėjo paskirti asmenys, dalyvaujantys Sutarties įgyvendinime, laikysis teisės aktuose numatytų asmens duomenų teisinės apsaugos reikalavimų ir įsipareigos saugoti asmens duomenų paslaptis perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams;

17.4.2. naudoti asmens duomenis laikantis galiojančių įstatymų, netvarkyti duomenų be dokumentuose užregistruoto Užsakovo Užsakymo, nebent tokia pareiga Tiekėjui numatyta pagal Europos Sąjungos arba valstybės narės įstatymus, taikomus tvarkymo subjektui;

17.4.3. saugoti, jog asmens duomenys nebūtų atskleisti neįgaliotiems asmenims, jog neįgalioti asmenys prie jų neprieitų, jie nebūtų perimti neįgalioto asmens, tvarkomi pažeidžiant galiojančių asmens duomenų apsaugos įstatymų nuostatas.

17.5. Tiekėjas įsipareigoja įgyvendinti tinkamas (atitinkančias Lietuvos ir Tarptautinių informacijos saugumo valdymo standartų reikalavimus) fizines, technines, programines ir organizacines priemones, skirtas konfidencialiai informacijai apsaugoti.

17.6. Tiekėjas bei jo paskirti asmenys, kurie sužino konfidencialią informaciją, gali ja naudotis tik tuo tikslu, dėl kurio ši informacija buvo atskleista, ir tik tiek, kiek būtina šalių bendradarbiavimui.

17.7. Tiekėjas naudojasi konfidencialia informacija taip, kad būtų užtikrintas Sutarties įsipareigojimų vykdymas, bei konfidencialia laikomos informacijos saugumas ir neprieinamumas tretiesiems asmenims.

17.8. Jeigu Tiekėjas sužino ar pagrįstai įtaria, kad konfidenciali informacija gali būti atskleista tretiesiems asmenims, jis įsipareigoja imtis visų įmanomų priemonių konfidencialiai informacijai apsaugoti.

17.9. Tiekėjas įsipareigoja nedelsiant pranešti Užsakovui, jeigu sužino arba pagrįstai įtaria, kad konfidenciali informacija buvo neteisėtai atskleista tretiesiems asmenims.

17.10. Nutraukus Sutartį arba įgyvendinus tikslą, dėl kurio konfidenciali informacija buvo atskleista, Tiekėjas privalo grąžinti visą konfidencialią informaciją Užsakovui sunaikinimui arba pats sunaikinti visą iš Užsakovo gautą konfidencialią informaciją, šiuo atveju Tiekėjas per 5 darbo dienas nuo Užsakovo pateikto prašymo gavimo dienos turi pateikti rašytinį patvirtinimą apie konfidencialios informacijos sunaikinimą, nurodant naudotas informacijos naikinimo priemones.

18.INTELEKTINĖS NUOSAVYBĖS TEISĖS

18.1. Visi rezultatai ir su jais susijusios teisės, įgytos vykdant Sutartį, įskaitant intelektinės nuosavybės teises į sukurtą Pirkimo objektą (Paslaugą) ar jo dalis, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus, yra Užsakovo nuosavybė (jeigu Sutarties SD nenurodyta kitaip), pereinanti

Užsakovui nuo Paslaugų rezultato perdavimo momento be jokių apribojimų, kurią Užsakovas gali naudoti, publikuoti, perleisti ar perduoti be atskiro Tiekėjo sutikimo tretiesiems asmenims neterminuotai, neapsiribojant teritorija, be jokių papildomų mokesčių.

18.2. Turtinės autorių teisės į Paslaugų teikimo metu sukurtus autorių teisių objektus Užsakovui perduodamos visam Teisės aktuose nustatytam autorių turtinių teisių galiojimo laikotarpiui nuo Akto pasirašymo momento.

18.3. Bet kokie su Sutartimi susiję dokumentai, išskyrus pačią Sutartį, yra Užsakovo nuosavybė ir, Tiekėjui baigus vykdyti savo įsipareigojimus, Užsakovo reikalavimu turi būti grąžinti (kartu su visomis jų kopijomis) Užsakovui, išskyrus dokumentus, kurie yra viešai prieinami ar kurie patvirtina Šalių mokėjimus.

18.4. Šios Sutarties tekstas, išskyrus Tiekėjo vienašališkai sudarytus dokumentus ir duomenis, identifikuojančius Tiekėją, yra Užsakovo autorinis kūrinys. Šios Sutarties sudarymo ir vykdymo procedūros yra Užsakovo geroji praktika. Tiekėjui suteikiama tik neišimtinė, terminuota teisė naudotis Sutarties tekstu tik šios Sutarties vykdymo tikslais. Bet koks kitoks šios Sutarties teksto ir (arba) patirties įgytos Užsakovui taikant Sutarties sudarymo ir vykdymo procedūras naudojimas Tiekėjo veikloje galimas tik gavus tam išankstinį rašytinį Užsakovo sutikimą.

18.5. Tiekėjas garantuoja nuostolių atlyginimą Užsakovui (įskaitant bylinėjimosi išlaidas) dėl bet kokių reikalavimų, kylančių dėl intelektinės nuosavybės teisių pažeidimo ar įtariamo jų pažeidimo (įskaitant gynybą įtariamo pažeidimo atveju), išskyrus atvejus, kai toks pažeidimas (įtariamas pažeidimas) atsiranda dėl Užsakovo kaltės.

18.6. Jeigu Sutarties vykdymo metu autorių teisių objektams sukurti Tiekėjas naudoja kitų autorių kūrinius ar Sutarties vykdymo metu numatytiems autorių teisių objektams sukurti Tiekėjo pasitelkiami kiti asmenys, Tiekėjas yra visiškai atsakingas tiek Užsakovui, tiek ir asmenims už jų kūrinių bei kitos medžiagos, skirtos Sutarties vykdymo metu numatytiems autorių teisių objektams gaminti (sukurti), naudojimo bei perdavimo Užsakovui teisėtumą. Tiekėjas prisiima atsakomybę už pretenzijas ar ieškinius, kylančius iš santykių su autoriais bei kitais trečiaisiais asmenimis dėl autorių teisių pažeidimo, susijusio su Sutarties vykdymo metu naudojamais ir (ar) Užsakovui perduodamais autorių teisių objektais ir įsipareigoja atlyginti Užsakovui jo dėl to turėtus nuostolius.

18.7. Tiekėjas nedelsdamas praneša Užsakovui apie tai, kad jam yra pateiktas ieškinys ar bet koks kitas reikalavimas dėl bet kokios su Sutartimi susijusios intelektinės nuosavybės teisės pažeidimo ar įtariamo pažeidimo.

18.8. Tiekėjas be išankstinio rašytinio Užsakovo sutikimo neturi teisės pagal Sutartį sukurtų autorių teisių objektų (įskaitant jų darbinius variantus) parduoti, bet kokiu kitu būdu perleisti, atskleisti tretiesiems asmenims, bet kokiu būdu platinti/demonstruoti šiuos objektus (jų sudedamąsias dalis) ir / ar bet kokiu kitu būdu naudotis Teisės aktuose nustatytomis autoriaus turtinėmis teisėmis į sutarties pagrindu sukurtus autorių teisių objektus (įskaitant jų darbinius variantus).

19. GINČŲ SPRENDIMO TVARKA

19.1. Kiekvieną ginčą, nesutarimą ar reikalavimą, kylantį iš Sutarties ar susijusį su Sutartimi, jos sudarymu, galiojimu, vykdymu, pažeidimu, nutraukimu, šalys spręs derybomis, vadovaudamosi Lietuvos Respublikos teisės aktais. Ginčo, nesutarimo ar reikalavimo nepavykus išspręsti derybomis, jie bus sprendžiami Lietuvos Respublikos teismuose pagal Užsakovo buveinės vietą.

20.UŽ SUTARTIES TINKAMĄ VYKDYMĄ ATSAKINGI ASMENYS

20.1. Už Sutarties tinkamą vykdymą Tiekėjo skirtas asmuo nurodytas Sutarties SD.

20.2. Už Sutarties tinkamą vykdymą Užsakovo skirtas asmuo nurodytas Sutarties SD.

20.3. Už Sutarties ir jos pakeitimų paskelbimą pagal Įstatymo 86 straipsnio 9 dalies nuostatas, Užsakovo skirtas atsakingas asmuo nurodytas Sutarties SD.

21. BAIGIAMOSIOS NUOSTATOS

21.1. Sutarčiai ir visoms iš šios Sutarties atsirandančioms teisėms ir pareigoms taikomi Lietuvos Respublikos įstatymai bei kiti norminiai teisės aktai. Sutartis sudaryta ir turi būti aiškinama pagal Lietuvos Respublikos teisę.

21.2. Visus kitus klausimus, kurie neaptarti Sutartyje, reguliuoja Lietuvos Respublikos teisės aktai.

21.3. Tiekėjas neturi teisės perleisti visų arba dalies teisių ir pareigų pagal Sutartį jokiai trečiajai šaliai be išankstinio raštiško kitos šalies sutikimo.

21.4. Šalys supranta ir patvirtina, kad Sutarties ir Sutarties priedų sąlygos nelaikomos konfidencialia informacija, jeigu konkrečiuose dokumentuose nenurodyta kitaip. Šalys laiko paslaptyje savo kontrahento darbo veiklos principus ir metodus, kuriuos sužinojo vykdant Sutartį, išskyrus atvejus, kai ši informacija yra vieša arba turi būti atskleista įstatymų numatytais atvejais.

21.5. Sutarties SD pasirašantys šalių atstovai patvirtina, kad Sutartis sudaryta be ekonominio spaudimo, laisva Sutarties šalių valia, ją pasirašantys Sutarties šalių atstovai Sutartį perskaitė, suprato jos turinį, pasekmes ir jos sudarymas visiškai atitinka šalių valią ir tikslus.

TECHNICAL SPECIFICATION FOR THE PUBLIC PROCUREMENT OF SERVICES

I part of the procurement object

1. DEFINITIONS AND ABBREVIATIONS	
1.1. DB	Database
1.2. IS	Information system
1.3. SW	Software
1.4. Procurement	A public procurement being carried out by the Contracting Authority for the procurement of the procurement object specified in this Technical Specification
1.5. Project	Project "Development of the national system for archiving and exchanging medical images and the electronic services it provides"
1.6. MedVAIS	National system for archiving and exchanging medical images
1.7. Contracting Authority, Buyer, Customer	The State Enterprise Centre of Registers, legal entity code 124110246, address Studentų St. 39, 08106 Vilnius. The Contracting Authority is a VAT payer
1.8. Contract	The Contract for the Public Procurement-Sale of Services awarded to the successful Provider (Supplier)
1.9. Provider (Supplier), deployer	A person (a natural person, a private legal entity, a public legal entity, other organisations and their units) or a group of persons with whom the Contracting Authority concludes a Contract
1.10. Technical Specification	Technical Specification for the Procurement
1.11. VNA	Vendor Neutral Archive
1.12. DICOM	ISO 12052:2017 standard Digital Imaging and Communications in Medicine.
1.13. Other definitions used in this Technical Specification are defined in the Contract, the Conditions of the Procurement, the Law on Public Procurement of the Republic of Lithuania, the Law on Public Procurement in the Field of Defence and Security of the Republic of Lithuania, the Procedure for low-value procurement, approved by Order No 1S-97 of the Director of the Public Procurement Office of 28 June 2017 on Approval of the Procedure for Low-Value Procurement, the Methodology for calculating the estimated value for the public procurement and procurement, approved by Order No 1S-94 of the Director of the Public Procurement Office of 27 June 2017 on Approval of the Methodology for Calculating the Estimated Value for the Public Procurement and Procurement, the Civil Code of the Republic of Lithuania and other legal acts regulating public procurement.	
2. GENERAL PROVISIONS	
2.1. For the purposes of this Technical Specification, the definitions "must be", "must have", "shall allow", "shall be able to", "will be", "will allow", "will include" are equivalent and mean that the Provider (Supplier) shall develop and implement (or provide and implement) the relevant functionality or provide relevant services within the scope of this procurement.	
2.2. Where specific models or sources, standards, certificates, protocols, concrete processes or trademarks, patents, types, specific origin or manufacture are mentioned in the Technical Specification when describing the procurement object, this shall include equivalent products or processes (i.e. the Provider (Supplier) may also offer relevant equivalent products or processes), regardless of whether these references are accompanied by the words "or equivalent" (the condition does not apply if the source, standard, certificate, protocol, concrete process or trademark, patent, type, specific origin or	

manufacture is mentioned in the definition of the products or existing processes held by the Contracting Authority or partners). The burden of proving equivalence lies with the Provider (Supplier). Minimum requirements have been laid down. Providers (Suppliers) may offer a procurement object with better characteristics.

2.3. General requirements for the provision of services:

2.3.1. The Provider (Supplier) shall provide the means and technical equipment necessary for the provision of the services;

2.3.2. The Provider (Supplier) shall not use third-party components that are new, have never been used in projects, are in Alpha or Beta testing and require additional run-time licences;

2.3.3. The Provider (Supplier) undertakes to provide written and oral advice to the representatives of the Contracting Authority in relation to the procurement object throughout the entire period of validity of the Contract;

2.3.4. The Contracting Authority undertakes to provide the Provider (Supplier) with the necessary and appropriate information for the proper performance of the Contract throughout the entire period of validity of the Contract;

2.3.5. Before granting access to personal data processed by the Contracting Authority, the Provider (Supplier) will be required to provide the Contracting Authority with the name, surname and contact details (telephone number, e-mail address) of the person responsible for the protection of personal data;

2.3.6. The Provider (Supplier) will be required to sign an agreement on the processing of personal data as set out in Article 28(3) of 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) (hereinafter referred to as the Regulation), which must set out the subject-matter and duration of the processing of personal data, the nature and purpose of the processing of data, the type of personal data and categories of data subjects, and the obligations and rights of the Centre of Registers;

2.4. The provision of the services must be carried out in accordance with the following legal acts and amendments thereto arising during the provision of the services, and other documents relating to the area of activity to be computerised and to the e-services to be developed or modified:

2.4.1. General Data Protection Regulation (EU) 2016/679;

2.4.2. Law on Public Procurement of the Republic of Lithuania;

2.4.3. Law on Public Procurement in the Field of Defence and Security of the Republic of Lithuania;

2.4.4. Law on Management of State Information Resources of the Republic of Lithuania;

2.4.5. Law on Legal Protection of Personal Data of the Republic of Lithuania;

2.4.6. Law on Cyber Security of the Republic of Lithuania;

2.4.7. Resolution No 349 of the Government of the Republic of Lithuania of 15 May 2024 on Implementation of the Law on Management of State Information Resources of the Republic of Lithuania;

2.4.8. Resolution No 478 of the Government of the Republic of Lithuania of 26 April 2001 on Approval of the Procedures to be Followed in Planning, Adjusting, Using, Accounting for and Controlling Public Funds Allocated for Public Capital Investments;

2.4.9. Description of Organisational and Technical Cybersecurity Requirements for Cybersecurity Entities, approved by the Resolution No 818 of the Government of the Republic of Lithuania of 13 August 2018 on Approval of the National Cyber Security Strategy;

2.4.10. Methodology for Lifecycle Management of State Information Systems, approved by Order No T-29 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications of 25 February 2014 on Approval of the Methodology for Lifecycle Management of State Information Systems;

2.4.11. Methodological recommendations for the development, testing and evaluation of websites of state and municipal institutions and bodies tailored for persons with disabilities, approved by the Order No T-72 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications of 23 May 2013 on Approval of the Methodological Recommendations for the Development, Testing and Evaluation of Websites Tailored for Persons with Disabilities; 2.4.12. Description of the national procedure for disclosure of communication and information systems vulnerabilities, approved by the Order No V-484 of the Minister of National Defence of the Republic of Lithuania of 9 July 2021 on Approval of the Description of the National Procedure for Disclosure of Communication and Information Systems Vulnerabilities.	
2.5. The Provider (Supplier) must comply with the legal acts in force at the time of performance of the Contract. The Provider (Supplier) shall also be bound by any newly adopted/amended legal acts during the performance of the Contract, insofar as it relates to the performance of the Contract. If newly adopted/amended legal acts are contrary to the requirements described in this Technical Specification, the Provider (Supplier) must implement the requirements in accordance with the current version of the adopted/amended legal acts at the time of performance of the Contract.	
2.6. The Provider (Supplier) shall be responsible for complying with the requirements of legal acts on occupational health and safety and other documents governing occupational health and safety in force in the Republic of Lithuania.	
3. PROCUREMENT OBJECT	
3.1. Procurement object	Implementation and configuration of VNA and DICOM based services (hereinafter referred to as the **Services**). The detailed requirements for the Services shall be specified in the Annex 'Requirements for the Procurement Object' to the Technical Specification (if applicable)
3.2. Division of the procurement object	The procurement object shall not be divided into lots. The reasons for non-division are set out in point 3.3.
3.3. Justification for not dividing the procurement object into lots (if applicable)	The procurement object cannot be divided into lots because of: 1) **Technical reasons** – The procurement object concerns the provision of one type of service, i.e. implementation and configuration of VNA and DICOM based services that are closely related to the functionalities developed by MedVAIS. The solutions chosen for the development and integration of new functionalities must be technologically aligned with each other, and when the Procurement Object is divided into parts and different suppliers develop the same IS, the solutions used by one supplier may be incompatible (or difficult to reconcile) with the solutions used by another supplier; 2) **Excessive time costs** – by dividing the procurement object into parts and developing the same IS by different suppliers, suppliers should, before starting to provide their share of services, receive the results of the provision of services of other suppliers and familiarize themselves with them, which would significantly increase the deadlines for achieving the final result and would risk the smooth and uninterrupted work of IS. Coordination between two or more suppliers would lead to significantly higher time costs for the coordination of decisions and processes for the Contracting Authority, as well as potentially affect the increase in the duration of the tasks, which could delay the

	delivery of the final result. 3) **Additional costs** – the coordination of the work of different suppliers and the delimitation of their responsibilities would entail additional administrative costs. In view of the fact that the supplier might also be settled at an hourly rate, any additional functions performed by the supplier, such as additional analysis, cooperation and/or planning and coordination of the services provided with other suppliers, would increase the working time for the performance of tasks, for which the Contracting Authority would have to pay additionally, at an hourly rate. Familiarizing different suppliers with the specifics of the project, the ESPBI IS architecture, and the needs of users would entail additional costs. Also, each supplier would have to do part of the analysis or preparation work anew, which would lead to double payment for the same processes.
3.4. Unit of measure	Kit Hour Month
3.5. Quantity (volume) of the Services	1 Kit (systems installation and configuration) Up to 300 hours (order of additional services) 60 months. System maintenance services
3.6. The specified quantity (volume) of the Services is	A maximum Services will be procured depending on the need, up to the maximum quantity indicated
3.7. Minimum quantity (volume) of the Services that the Contracting Authority undertakes to procure during the performance of the Contract (if applicable)	1 Kit
3.8. Changing the quantity (volume) of the Services	Not applicable
3.9. Place of delivery of the Services	The Services shall be provided remotely or, if necessary, at the Contracting Authority's premises located at Studentų St. 39, Vilnius. Place of delivery of the Services may be changed within the limits of Vilnius city.
3.10. Term for delivery of the Services	3.10.1. Services must be provided no later than within 7 months from the date of entry into force of the Agreement (in case there are at least 7 months left on the date of contract until 30.04.2026) or until 30.04.2026 (in case there are less than 7 months left on the date of the contract until 30.04.2026). 3.10.2. Additional Services must be provided from the date of entry into force of the Agreement for 7 months (in case there are at least 7 months left on the date of the contract until 30.04.2026) or until 30.04.2026 (in case there are less than 7 months left on the date of the contract until 30.04.2026). Service Orders may be placed and must be fulfilled within the time period specified in the Order, but no

	later than the expiry term/date specified above. 3.10.3. Maintenance services will have to be provided (if ordered) for the period ordered, up to a maximum of 60 months. The maintenance services shall not commence before the expiry of the warranty period and shall be ordered by the Contracting Authority.
3.11. Extension of the term of delivery of the Services and conditions	3.11.1. The term for the delivery of services referred to in Clause 3.10.1 may be extended if: 3.11.1.1. there are evidence based obstacles or disruptions, the occurrence of which is not influenced by the Parties and for which they are not responsible, and which are caused and attributable to third parties, or other circumstances which the Parties could not have foreseen in advance. The circumstances on which the need to extend the term of provision of the Services is based can in no way depend on the parties to the Agreement. In each such case, the Contracting Party initiating the extension of the term of provision of the Services shall, without delay in writing, but not later than within 5 working days, notify the other Contracting Party thereof, providing evidence of the existence of the aforementioned circumstances. The indicated circumstances shall be assessed by the other party to the Agreement, upon the latter's consent, the term of provision of the Services may be extended only for the period of existence of the aforementioned circumstances, but not longer than: 3.11.1.1.1. until 30.04.2026; or 3.11.1.2 for the deadline for the implementation of the project, if the deadline for the implementation of the project will be extended, but not longer than for a period of 6 months; or 3.11.1.3. for a period of no longer than 6 months in case funding will be allocated outside the Project. 3.11.2. The deadline for the provision of additional services specified in 3.10.2. may be extended if the Initial Value of the Contract is not used. In such a case, the Contracting Authority shall notify the Provider in writing, indicating the term for which it is proposed to extend the term of provision of the Services. With the Provider's consent, the term of provision of Services may be extended only until the Initial Value of the Contract is exhausted, but not longer than for a period of 6 months (the number of extensions is not limited).
. OBLIGATIONS OF THE PROVIDER (SUPPLIER)	
4.1. Time limit for the Provider (Supplier) to inform the Customer in writing of any circumstances which hinder and/or may prevent the Provider (Supplier) from fulfilling its contractual obligations in	5 working days

accordance with the terms and conditions set out in the Contract	
4.2. Other obligations of the Provider (Supplier)	-
4.3. Other obligations of the Provider (Supplier) shall be specified in the Annex 'Requirements for the Procurement Object' to the Technical Specification (if applicable), the draft Contract and the Procurement Conditions	
. PROCEDURE FOR TRANSFER AND ACCEPTANCE OF THE SERVICES	
5.1. Deadline for signing the Statement	5 working days
5.2. Periodicity of signing the Statement	5.2.1. The Statement shall be signed after each phase specified in the II Part 'Requirements for the Procurement Object' to the Technical Specification. 5.2.2. The actual quantities of the additional services provided are forwarded to the Customer when the Parties sign the Statement of Additional Service Provision during the previous month. The Statement is signed once a month.
6. QUALITY OF THE SERVICES	
6.1. Guarantee term of the Services	12 months
6.2. Deadline for removal of Service deficiencies observed during the transfer - acceptance of the Services and/or after the signing of the Statement	10 working days from sending a notification of the deficiencies observed
7. REQUIREMENTS RELATING TO NATIONAL SECURITY	
7.1. In order to avoid security gaps and vulnerabilities in the software, the Provider (Supplier) must follow generally accepted secure coding standards and good practice (The Open Web Application Security Project (OWASP) Secure Coding Practices, etc.) for the development of the SW and the provision of SW maintenance services. The developed SW must be free of unauthorised access to data and other security vulnerabilities listed in the latest OWASP Testing Guide (not limited to the OWASP Top 10 vulnerabilities) (https://www.owasp.org), The OWASP API Security Checklist, and other IS security methodologies developed by OWASP or equivalent documents. Security checks (threat modelling, source code reviews, and other security checks required by secure coding standards and good practice) must be carried out at every stage of SW design (development, maintenance). The security checks must be based on the latest versions of the following methodologies: OWASP Web Security Testing Guide, Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), SANS, NIST SP 800-30 or equivalent security check methodologies.	
7.2. The Provider (Supplier) must, in agreement with the Contracting Authority, use the latest versions of SW packages, libraries, programming languages, their compilers and interpreters available at the time of development of the newly created SW.	
8. ENVIRONMENTAL REQUIREMENTS	
8.1. Given that the Services procured are intangible intellectual services not related to the creation of a tangible object, the provision of which will not create negative environmental effects, nor will it create a source of pollution or generate waste, in accordance with the Procedure for Applying Environmental Criteria in Green Procurement approved by the Order No D1-508 of the Minister of Environment of the Republic of Lithuania of 28 June 2011, the Procurement shall be considered green.	
9. HIERARCHY	
9.1. This Technical Specification shall be an integral and indivisible document.	

9.2. The following order of priority of the Procurement documents shall be established for the purposes of interpretation and invocation of the Technical Specification:
9.2.1. Tender notice;
9.2.2. Special Part of the Contract;
9.2.3. Technical Specification;
9.2.4. Annex No. 1 'Requirements for the Procurement Object' to the Technical Specification (if applicable);
9.2.5. Other Annexes to the Technical Specification (if applicable);
9.2.6. General Part of the Contract;
9.2.7. Procurement Conditions;
9.2.8. Annexes to the Procurement Conditions;
9.2.9. Tender bid.
9.3. If any of the documents referred to in point 9.2 contains ambiguities, inconsistencies, or contradictions with the conditions set out in a higher-ranking document, these shall always be deemed to prevail over the conditions set out in the lower-ranking document from the moment they are established.
9.4. In the event the documents submitted by the Provider (Supplier), including licences, rules for their use, etc., contradict the conditions set out in the documents referred to in points 9.2.1 to 9.2.8, the provisions of the documents referred to in points 9.2.1 to 9.2.8 shall apply.

10. ALONG WITH THE TENDER BID, THE PROVIDER (SUPPLIER) MUST SUBMIT

10.1. Recommendations on the minimum infrastructure requirements for new system and medical image storage. It must include:
- Recommendations shall be made for different segments of the system usage: volume of medical images per year – 1, 2 and 5 million studies per year; number of concurrent DICOM viewer users – 50, 100 and 300.
- Planned number of servers, their purpose (application and database servers) and resources required (CPU, RAM, Memory).
- Technical requirements for medical image storage technologies.
- Minimum and recommended requirements should be identified where possible.
- Other information that might be useful in planning infrastructure for the new systems and medical image storage.

11. ANNEXES

11.1. Annex No. 1	Requirements for the procurement object

Procurement Conditions for
IS Modernization Services
Technical Specifications
Annex 1

REQUIREMENTS FOR PROCUREMENT OBJECT
I PART OF THE PROCUREMENT OBJECT
NATIONAL MEDICAL IMAGE ARCHIVING AND EXCHANGE INFORMATION SYSTEM
MODERNIZATION SERVICES

Content

1. PROJECT GOALS AND OBJECTIVES 3
1.1. Summary 3
1.2. Terms and abbreviations 3
1.3. Legal acts regulating the modernization and operation of the information system and the provision of services 4
1.4. Procurement objectives 6
1.5. Issues to be addressed 7
2. DESCRIPTION OF CURRENT SITUATION 7
2.1. Organizational structure of the system 8
2.2. System users and target groups 8
2.3. Functional structure of the system 9
2.3.1. System logical model 10
2.3.2. Used technologies 14
2.4. System file structure 15
3. DESCRIPTION OF THE DESIRED STATE OF THE SOLUTION 15
4. DESCRIPTION OF FUNCTIONAL REQUIREMENTS 17
4.1. General requirements 17
4.2. Functional requirements 19
5. NON-FUNCTIONAL REQUIREMENTS 23
5.1. Criteria for the implementation of non-functional requirements 23
5.2. Requirements for the System architecture 23
5.3. Requirements for medical image viewer 24
5.4. Requirements related to the data register and storage management tool (hereinafter referred to as the "Tool"): 25
5.5. Requirements for technology 25
5.6. Requirements for system availability 26

5.7. Requirements for scalability 26
5.8. Requirements for the creation and restoration of backup copies....27
5.9. Requirements for system monitoring 27
5.10. Requirements for a data model 28
5.11. Requirements for system administration....29
5.12. Requirements for performance and speed 29
5.13. Requirements for software and software licenses....31
5.14. Requirements for integrations 33
5.15. Requirements for user interface and ease of use....33
5.16. Requirements for data archiving 34
5.17. Requirements for the application of standards 34
6. REQUIREMENT FOR SERVICE PROVISION....35
6.1. Requirement for workplace 35
6.2. Requirements for ordering services....36
6.3. Requirements for the implementation of the RPO 36
6.4. Requirements for service stages and software development iterations 39
6.4.1. Requirements for documentation and its coordination....48
6.4.2. Requirements for analysis and design....49
6.4.3. Requirements for demonstrations....49
6.4.4. Requirements for deployment....50
6.4.5. Requirements for testing 51
6.4.6. Requirements for training....53
6.4.7. Requirements for pilot testing....54
6.5. Requirements for acceptance of the System 55
6.6. Requirements for warranty 56
6.7. Requirements for Project management 57
6.8. Requirements for change management....58
6.9 Requirements for maintenance....59
7. SPECIAL REQUIREMENTS FOR THE PROVISION OF SERVICES....63
7.1. Safety requirements....63
7.1.1. Requirements for data protection and information security management....63
7.1.2. Requirements for the application of safety legislation....64
7.1.3. Data security requirements for the provision of services....65
7.1.4. Requirements for audit records....66
7.1.5. Requirements for risk, threat and vulnerability management 67
7.1.6. Requirements related to national security 67
7.1.7. Other security requirements 68
8. Annexes 70
8.1. Annex 1. Order form for additional services....70

1. PROJECT GOALS AND OBJECTIVES

1.1. Summary

1. Requirements according to which the National medical image archiving and exchange information system (hereinafter referred to as the MedVAIS or the System) is to be modernized are presented.
2. RPO provides information on the legal acts and standards to be followed by the System modernization service Provider during the modernization of the System. It identifies the Procurement tasks, provides the intended functional architecture of the System and its description, describes the state to be achieved and specifies functional and non-functional requirements when modernizing the System.
3. This part of procurement object includes:
3.1 Ensure DICOM standard implementation by enabling DICOM and non-DICOM image and metadata management through DICOMweb (e.g. QIDO-RS, WADO-RS, STOW-RS) and DIMSE (e.g. C-FIND, C-MOVE, C-STORE) protocols.
3.2 Integration of DICOM viewer, enabling medical image viewing for users.
3.3 Vendor neutral archive integration – standard medical image and related information transfer and storage independent from vendor or specific diagnostic equipment.

1.2. Terms and abbreviations

4. RPO terms and abbreviations are presented in table 1 „Terms and abbreviations".

Table 1. Terms and abbreviations

Term/abbreviation	Description
PHCI	Personal health care institution
ESPBI IS	Electronic information system of health services and cooperation infrastructure
Project	Development of the National System for the Archiving and Exchange of Medical Images (MedVAIS) and the electronic services it provides
RC, Contracting Authority	State Enterprise Centre of Registers
Service provider	Company that is providing services for the implementation of the project according to this technical specification.
SAM	Ministry of Health of the Republic of Lithuania
IS	Information system
SW	Software
HW	Hardware
Portal or e. health portal	A way for authenticated patients and healthcare specialists to access electronic services via web. In the ESPBI IS environment, the Portal is implemented by the eHealth Portal Subsystem (hereinafter referred to as the eHealth Portal Subsystem).
XML	Extensible Markup Language

Term/abbreviation	Description
DICOM	Digital Imaging and Communications in Medicine. Standard (ISO 12052:2017) describing the processing, storage and exchange processes of digital medical images and related information.
FHIR	Fast Healthcare Interoperability Resources.
MedVAIS or System	National medical image archiving and exchange information system
PACS	Picture Archiving and Communication System.
HIS	Hospital information system
RIS	Radiology Information System.
UID	Unique Identifier described in DICOM standard.
EHR	Electronic Health Record

5. Other terms used in the RPO are defined in the following legal acts.

1.3. Legal acts regulating the modernization and operation of the information system and the provision of services

6. Law on the health System of the Republic of Lithuania.
7. Law on Health Insurance of the Republic of Lithuania.
8. Law on Legal Protection of Personal Data of the Republic of Lithuania.
9. Law on Cybersecurity of the Republic of Lithuania.
10. Description of the procedure for using the information system of the electronic health services and cooperation infrastructure, approved by Order No V-657 of the Minister of Health of the Republic of Lithuania of 26 May 2015 "On the approval of the description of the procedure for the use of the information system of the Electronic Health Services and Cooperation Infrastructure".
11. Regulations of the Electronic Health Services and Cooperation Infrastructure Information System, approved by Resolution No. 1057 of the Government of the Republic of Lithuania of 7 September 2011 "On the Approval of the Provisions of the Information System of the Electronic Health Services and Cooperation Infrastructure".
12. Requirements and technical conditions for linking the information systems of health care institutions to the Electronic Health Services Cooperation and Infrastructure Information System, approved by Order No V-1079 of the Minister of Health of the Republic of Lithuania of 17 December 2010 "On the approval of the requirements and technical conditions for linking the information systems of health care institutions to the Electronic Health Services Cooperation and Infrastructure Information System".
13. The model of the functional, technical, and software architecture of the Lithuanian e-Health system, approved by the Minister of Health of the Republic of Lithuania on October 2, 2019, by Order No. V-1119 "On the Approval of the Functional, Technical, and Software Architecture of the Lithuanian e-Health System.".
14. Order of the Minister of Health of the Republic of Lithuania of 4 July 2018 No V-769 "On the approval of the description of the procedure for the implementation of the rights of data subjects in the electronic health services cooperation and infrastructure information system".

15. Order No. 515 of the Minister of Health of the Republic of Lithuania of 29 November 1999 on the „Accounting and Reporting Procedures for the Activities of Healthcare Institutions".
16. Law on the Management of State Information Resources of the Republic of Lithuania.
17. ESPBI IS regulations shall be adjusted in accordance with the Description of the Procedure for the Establishment, Development, Renewal, Reorganization and Liquidation of Information Systems, approved by Resolution No. 349 of the Government of the Republic of Lithuania of 15 May 2024 "On the Implementation of the Law on the Management of Information Resources of the State of the Republic of Lithuania".
18. The technical description (specification) of the ESPBI IS is prepared after the approval of the updated ESPBI IS regulations. The technical description (specification) of ESPBI IS is prepared in accordance with the Description of the Procedure for the Establishment, Development, Renewal, Reorganization and Liquidation of Information Systems, approved by Resolution No. 349 of the Government of the Republic of Lithuania of 15 May 2024 "On the Implementation of the Law on the Management of Information Resources of the State of the Republic of Lithuania".
19. Methodology for the Management of the Life Cycle of State Information Systems, approved by Order No. T-29 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications on February 25, 2014, "On the Approval of the Methodology for the Management of the Life Cycle of State Information Systems".
20. Methodology for the development of electronic services, approved by Order No. 3-416(1.5E) of the Minister of Transport and Communications of the Republic of Lithuania of 7 October 2015 "On approval of methodological documents".
21. Recommendations for Data Provision Formats and Standards, approved by Order No. T-36 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications on March 25, 2013, "On the Approval of Recommendations for Data Provision Formats and Standards".
22. Methodological Recommendations for Ensuring User-Friendliness of Public and Administrative Electronic Services, approved by Order No. T-65 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications on May 5, 2014, "On the Approval of Methodological Recommendations for Ensuring User-Friendliness of Public and Administrative Electronic Services".
23. Technical Supervision Recommendations for Projects that Develop Electronic Services and IT Solutions, approved by Order No. T-126 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications on November 22, 2017, "On the Approval of Technical Supervision Recommendations for Projects that Develop Electronic Services and IT Solutions".
24. Methodological Recommendations for Creating and Testing Websites Adapted for People with Disabilities, approved by Order No T-40 of 31 March 2004 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications.
25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).
26. Description of Organizational and Technical Cybersecurity Requirements Applicable to Cybersecurity Entities, approved by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 on the Implementation of the Law on Cybersecurity of the Republic of Lithuania.

27. Information Technology Security Conformity Assessment Methodology, approved by Order No V-941 of the Minister of National Defense of the Republic of Lithuania of 4 December 2020 "On the approval of the Methodology for Conformity Assessment of Information Technology Security".
28. Technical Supervision Recommendations for Projects that Develop Electronic Services and IT Solutions, approved by Order No. T-126 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications on November 22, 2017, "On the Approval of Technical Supervision Recommendations for Projects that Develop Electronic Services and IT Solutions".
29. Other legal acts regulating the operation of state information systems, data security, and functions.
30. If, during execution of the Contract, listed or other legal acts related to the implementation of the requirements provided for in this Technical Specification are amended, the Service provider must take these changes into account, provided that they were known before the end of the design phase. If changes to the legislation were adopted, then it is considered that Service provider was obliged to know about such changes. If amendments to the legislation have not yet been adopted, but are only at the stage of preparation, consideration or adoption, the Service provider shall be deemed to have become aware of such changes only after the Contracting Authority has informed Service provider and requested to make changes according to the amendments.
31. Service provider must follow not only the above, but also all other legal acts related to the implementation of the Contract, as well as their latest amendments and additions. Service provider must follow the newly adopted legislation during the performance of the Contract, provided that they relate to the implementation of the Contract and are adopted no later than the end of the design phase.

1.4. Procurement objectives

32. Objectives:
32.1. Carry out a detailed analysis of needs and opportunities.
32.2. Model and design the functionality of the modernized ESPBI IS MedVAIS subsystem and data exchange interfaces.
32.3. Prepare and coordinate all the planned System documentation.
32.4. Realize the functions of the System and data exchange interfaces.
32.5. Implement system functions and data exchange interfaces.
32.6. Install databases and other necessary standard software.
32.7. Successfully perform validation testing of the functions and interfaces created by the System.
32.8. Prepare training materials and conduct training.
32.9. Prepare the System for operation.
32.10. Successfully perform a pilot testing of the created System.
33. The results of the services purchased:
33.1. Developed, implemented and tested modernized ESPBI IS with updated MedVAIS subsystem.
33.2. Developed interfaces with external information systems and registers.
33.3. System technical documentation prepared.
33.4. Trained System Users.
33.5. Provided warranty of the System.

1.5. Issues to be addressed

34. The architecture of MedVAIS is limited to the content of the medical images declared and submitted by a particular PHCI, there is no possibility to compile list of medical images created by several PHCI based on diagnoses, body areas or a specific patient. Data on medical images that are not declared and/or transferred for storage to MedVAIS is not available at national level, so there is no access to medical image data for the purpose of providing and re-using healthcare services.
35. Existing search parameters for medical images limit the possibilities of analytics arising from the different needs of health professionals.
36. There is no fully functional anonymization functionality, which would expand the possibilities of re-using medical imaging data.
37. It is not possible for a user to view medical images stored in MedVAIS repository without having own viewer and PHCI doctors cannot download the diagnostic tests generated by their ASPI to their workstations through the eHealth Portal.
38. The existing report of medical images is not structured, i.e. the data fields are not connected with the classifiers and the values of the variables unified in them, which unreasonably prolongs the processes of creating it.
39. The existing report does not contain all the fields specified in the European Commission's recommendations that are used to query reports and medical images.
40. Currently, MedVAIS uses the ESPBI IS user access rights to the EHR records module for patients' access rights to patients. This module is not suitable in practice in ordinary situations of medical imaging: medical image is created by specialists of one PHCI, and report is prepared by the radiologist of another PHCI. Currently, MedVAIS medical image can only be approved by declaring/transmitting the image and report together, i.e. authorizing from one PHCI. It is therefore necessary to upgrade MedVAIS by creating a user rights management algorithm adapted to the normal situation in practice.
41. Currently, not all types of medical images created during the provision of health care services are stored in MedVAIS: for example, jpg, which are important for doctors-dermatologists, as well as blood pressure measurements, data carried out by HOLTER machines, sleep monitoring data, and so on are not stored.

2. DESCRIPTION OF CURRENT SITUATION

42. National medical image archiving and exchange IS MedVAIS was developed in 2013-2015 as a separate ESPBI IS subsystem for storing, archiving and sharing medical images among PHCI:
42.1. MedVAIS has accumulated 24 types of digital medical imaging results from radiological, ultrasound and ECG examinations.
42.2. According to data from Institute of Hygiene, together x-ray (XA), ultrasound (US), computed tomography (CT), magnetic resonance (MR), endoscopy (ES) and positron emission tomography (PT) account for approximately 6 million studies per year. Total size of studies per year in Lithuania is ~ 600 Tb and 20 – 25 % of it is sent to MedVAIS (size estimated considering XA – 90 Mb, US – 60 Mb, CT – 430 Mb, MR – 115 Mb, ES – 30 Mb, PT – 30 Mb).
42.3. Each year approximately 1,8 million images are sent to MedVAIS. It is from few to ~ 40 % of total number of images in the years 2015 – 2023.

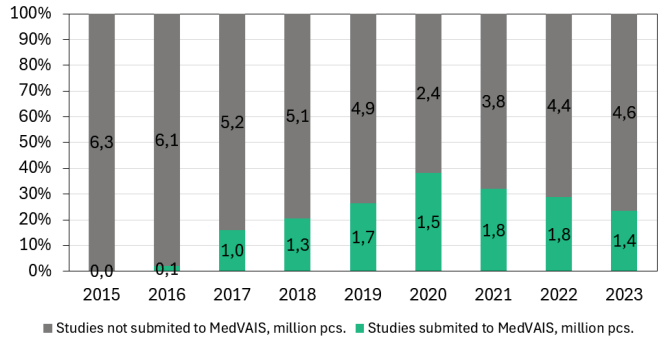


Figure 1. Number of medical images in MedVAIS and Lithuania through 2015 – 2023.

42.4. By the end of 2023, more than 15 million medical images were stored in MedVAIS. The total size of stored medical images in MedVAIS at the end of 2024 was 1.4 PB, while the total capacity of the infrastructure for the storage – 2.3 PB.
42.5. Each medical image is associated with a separate EHR record, i.e. the data set E027-va "Diagnostic description of the medical image", the structure of which is given in table no. 3.
42.6. Currently there are over 11 million signed reports submitted to MedVAIS.

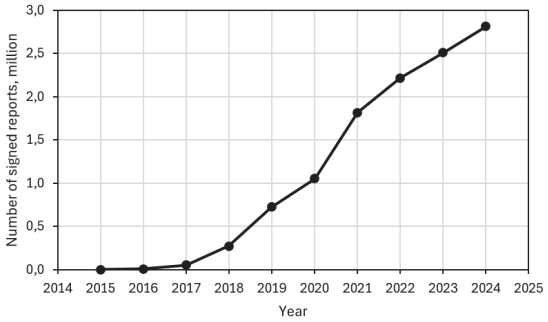


Figure 2. Signed reports submitted to MedVAIS through 2015 – 2024.

42.7. Currently, there are ~ 200 healthcare facilities integrated into MedVAIS (PACS sends medical images to MedVAIS).
42.8. MedVAIS was designed to provide the following capabilities:
42.9. For PHCI and professionals electronically obtain the results of diagnostic imaging of other PHCI.
42.10. For PHCI, which created the medical image, submit a medical image electronically for the analysis of another PHCI specialist, through the e-health portal.
42.11. View medical images in MedVAIS for patients, healthcare professionals, organizations involved in the management and control of healthcare services.
42.12. Receive and view statistical reports and data.
42.13. Get an anonymized medical image for the management and control of health care services and scientific activities.

2.1. Organizational structure of the system

43. The system controller is the Ministry of Health of the Republic of Lithuania, the System Processor is RC.

2.2. System users and target groups

44. Description of system users is provided in table 2.

Table 2. Description of system users

No.	User	Description
1.	Patient	A person who uses the services provided by health care institutions, regardless of whether he is healthy or sick.
2.	Health Care Specialist	A person providing health care services – a family doctor, or a doctor of any other specialization (except for specialist who perform and report on radiological, ultrasound, ECG and EEG examinations) who can review the patient's health history, prepare examination orders. This role does not give the right to prepare diagnostic descriptions of medical images.
3.	Radiologist	A radiologist who reviews the medical radiological images created by the devices, makes annotations to medical images, creates reports and has the right to sign them. In the case of diagnosis of ultrasound, ECG and EEG tests, the concept of "Radiologist" is conditionally expanded to include other specialist doctors who have the right to diagnose the relevant examinations.
4.	PACS	Picture archiving and communications system
5.	HIS	Hospital information system
6.	RIS	Radiology information system
7.	Organizations coordinating and administering health care activities	Organizations coordinating and administering health care activities, which need MedVAIS data for the formation of health care policies.
8.	Organizations engaged in scientific activities	Organizations engaged in scientific activities for which MedVAIS data is needed for research purposes.

2.3. Functional structure of the system

45. ESPBI IS functional components referred in point IV of the ESPBI IS Regulations form the functional architecture and are described in the ESPBI IS logical model.
46. ESPBI IS is the main tool for the implementation of the digital health system of the Republic of Lithuania – the totality of organizational, telecommunication, software tools and databases for centralized creation, usage, storage of electronic personal health records and their exchange between institutions engaged in health promotion activities, their specialists and other employees. ESPBI IS ensures cooperation between the subjects of the Lithuanian digital health system and the integration of their information systems through the data exchange subsystem, operation of digital health services and access to the information resources of public administration institutions.

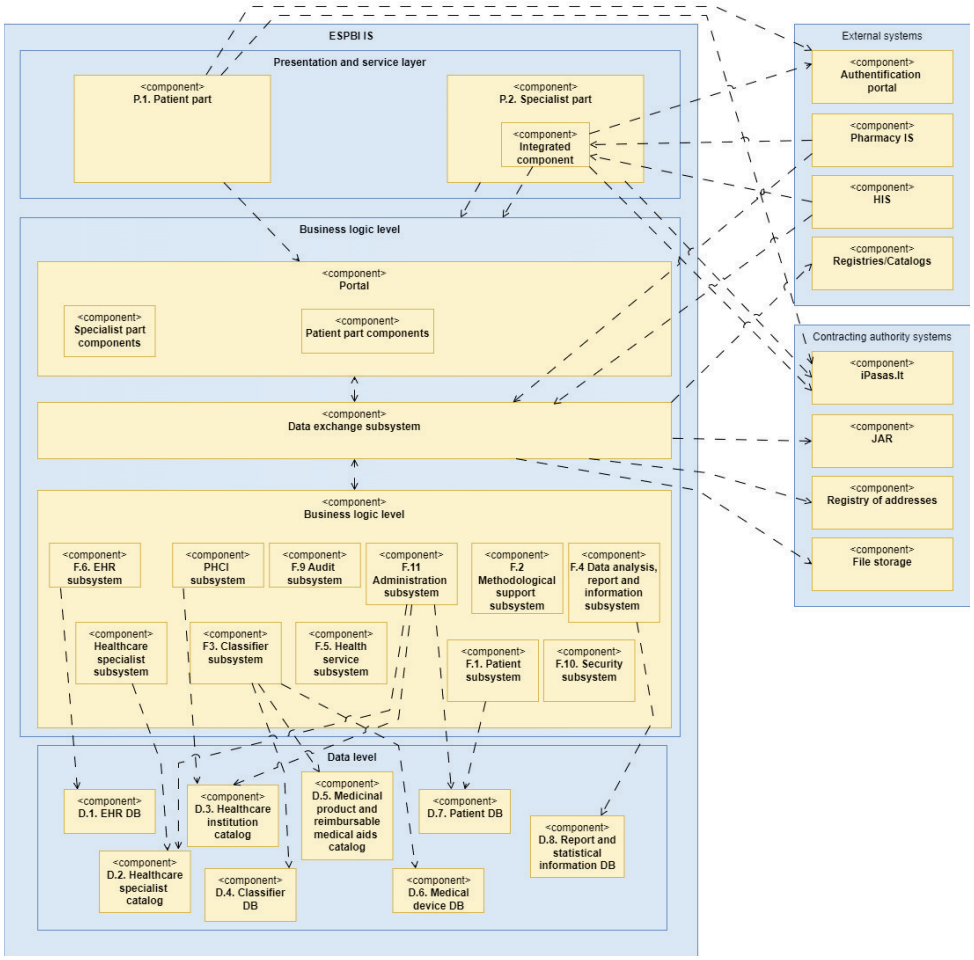


Figure 3. Digital Health System Architecture

2.3.1. System logical model

47. ESPBI IS subsystems:

- A subsystem providing access to e-services for patients and health professionals – The Digital Health Portal (hereinafter referred to as the Portal) – set of tools for implementing the principle of single window access for the residents, health care and pharmaceutical professionals.
- Authentication subsystem – by using VIISP (State Information Resources Interoperability Platform) or ESPBIS IS tools identifying the users of ESPBI IS, ensure the identification of users of the ESPBI IS, the identification of the users of the Portal, generate an electronic signature and allow the signing of electronic forms of documents with an electronic signature. Authentication of all ESPBI IS users is carried out through the VIISP user authentication module.
- Administration subsystem – ensures the management of ESPBI IS, effective tools for the administration of ESPBI IS and the monitoring of the technical (system) processes taking place in the ESPBI IS.
- Security subsystem – registers ESPBI IS users, grants and manages the data access permissions of ESPBI IS users, ensures the identification of ESPBI IS users and the identification of portal users through the VIISP, ensures the management of the permissions

of ESPBI IS users, ensures the security of ESPBI IS data, ensures the archiving of ESPBI IS data and the making of backup copies of data.

- Audit subsystem – ensures effective ESPBI IS monitoring and auditing tools, records all actions of ESPBI IS users, ensures the integrity of audit records and record retrieval, prepares reports on the actions of users of ESPBI IS.
- EHR subsystem – ensures the processing and retrieval of EHR data, the provision of patient data to the ESPBI IS data exchange and portal subsystems.
- Patient Subsystem – ensures the processing and retrieval of patients' general data, identification of the patient by name and date of birth, personal identification number, gender, EHR identification number.
- The classifier subsystem centrally processes the data of the classifiers, provides classification data to ESPBI IS processors, ESPBI IS data providers and other interested authorities, ensures the search for data in the classifiers.
- E-prescription subsystem – enables the electronic prescription of medicinal products and compensatory medical aids and collects data on them, manages data on prescriptions issued electronically, prepares and submits reports on prescribed medicinal products and compensatory medical aids, ensures the search for e-prescription data.
- Medical Imaging Subsystem (MedVAIS) – ensures the functioning of the national repository of medical images, manages medical images, ensures access to stored medical images and medical images for healthcare professionals and patients.
- Healthcare services subsystem – collects and provides data on the provided healthcare services, prepares and provides reports on the provided healthcare services reimbursed from the budget of the compulsory health insurance fund.
- Subsystem for the provision of methodological assistance to a health care specialist – provides information about recommended research, treatment methods, provides clinical information of medicinal products and other methodological information.
- Data analysis, reporting and information subsystem – provides reports according to predetermined indicators, ensures the implementation of data analysis in various sections using software analysis tools, ensures the preparation of disease and morbidity analysis and reports, prepares and submits statistical and public health monitoring reports and other reports necessary for the subjects of health promotion activity management, forms statistical and analytical reports from data from other subsystems, provide the public with publicly available statistical information.
- Data Exchange Subsystem – ensures the exchange of data between ESPBI IS and other components of the digital health system (information systems of institutions engaged in health promotion activities, health sector registers and information systems and other sectors of public administration), electronic medical history data exchange between the Mobile App and other data exchange components, as well as provides data from ESPBI IS classifications to health promotion institutions and interested institutions information systems.

48. MedVAIS subsystem:

- MedVAIS architecture is based on the creation of virtual PACS for each PHCI that sends or receives medical images to or from MedVAIS. PACS are created on separate virtual machines as DCM4CHEE application entities.
- DCM4CHEE is based on the principle of one DCM4CHEE application entity - one institution. As a result, a separate database schema is created for each institution, in which all stored data is treated by the PACS as the data of that institution.

- A secure VPN channel is used to establish and maintain the connection between the PHCI PACS and the MedVAIS PACS.
- The data model and functionalities in the MedVAIS subsystem consist of two logical areas: MedVAIS PACS and ESPBI IS MedVAIS.
- MedVAIS PACS includes the part of the system operation, where virtual PACS systems for working with PHCI devices are implemented and ensures DICOM communication. DCM4CHEE provides that each institution has its own dedicated database scheme, which is used by MedVAIS PACS. There are as many database schemas that are identical in structure as there are virtual PACS for institutions. This part collects the data that appears in the system during the communication with the DICOM protocol, as well as additional and auxiliary data.
- ESPBI IS MedVAIS data structure and functionality area covers all data structures that are realized in the ESPBI IS part. Since MedVAIS is an integral, unified ESPBI IS subsystem, components related to the operation of the Portal are implemented by the same means and principles as the central part of ESPBI IS, also implementing a unified data model. Therefore, the elements of medical image report and the medical image are realized as resources of the FHIR standard. The same data management principles are applied – the medical image report is constructed as a composition of FHIR resources, resource data is stored in the same database next to the resource data of the central part of ESPBI IS, resources references to the resources managed by the central part of ESPBI IS (resources of the patient, doctor, institution). The link between the two parts of the data is realized through the essence of the study. Medical image always has a unique UID, which is recorded both in the DCM4CHEE database and in the corresponding FHIR resource. The FHIR resource ImagingStudy also records other DICOM data, but the study's UID remains the main link between the data structures in both domains.

Integration with MedVAIS is based on two main principles for communication:

- Submitting and receiving medical images – DICOM communications with MedVAIS PACS. All communications and data transfer between institution PACS and MedVAIS PACS are done according to DICOM standard version 3.
- Reporting of medical images and other related documents – FHIR communication via ESPBI IS endpoints.

For each medical image, which is sent to MedVAIS in DICOM format, MedVAIS generates ImagingStudy FHIR resource. All further actions through eHealth portal or endpoints, where finding, creating report, viewing or other action with medical image is needed – relevant ImagingStudy resource is used. FHIR resource is linked with DICOM study by UID. General workflow for medical image report generation is provided in a figure below.

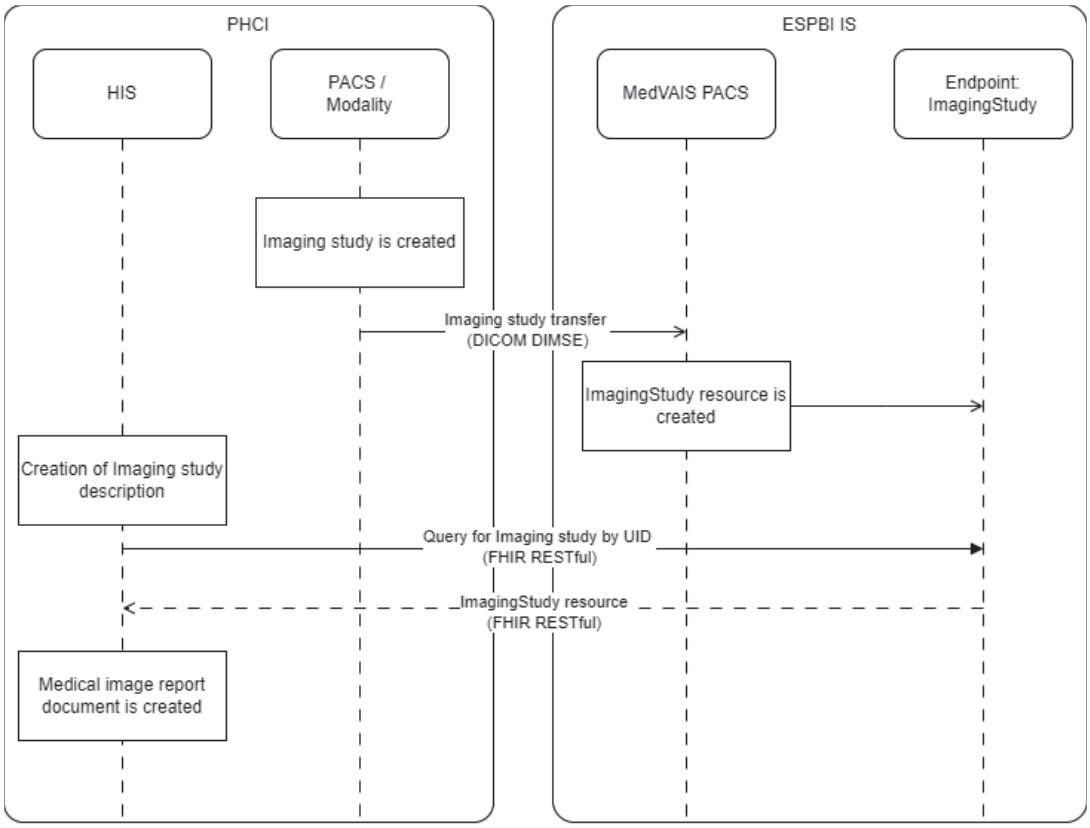


Figure 4. Example of integration for preparation of medical image report

Details of the medical image report generation and transfer to ESPBI IS is provided in a figure below. Medical image report is transferred to FHIR endpoints via FHIR RESTful protocol. In the provided example, "Sign medical document" component is responsible for signing and saving PDF document, corresponding to the dataset provided in Table 3 together with institution, patient and specialist data.

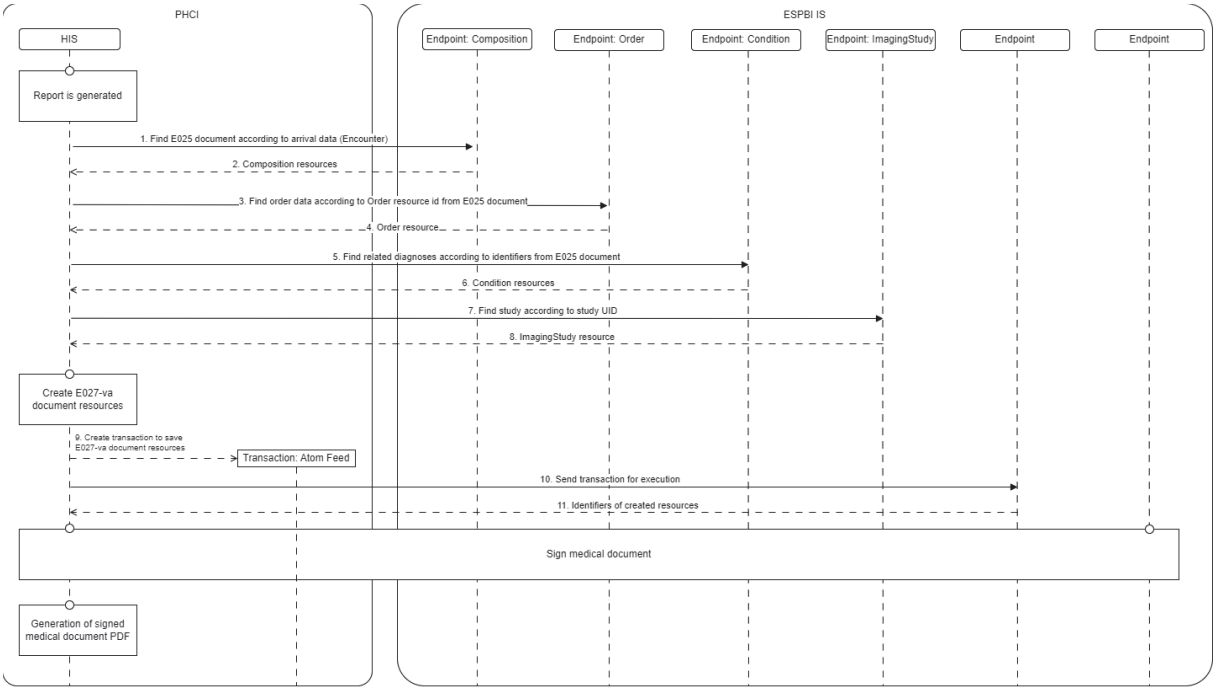


Figure 5. Scenario of E027-va report document submission

Interaction between institutions and MedVAIS is described in more details and provided in EPSBI IS data exchange and integration design documentation, chapter 3.15 "PHCI and MedVAIS integration documentation" (lith. SPĮ ir MedVAIS integracijos dokumentacija)[1].

Table 3. Medical image report dataset

No.	Field	FHIR resource	Attribute
10.1.	**Order details:**		
10.1.1.	Came with an order (YES / NO):	Encounter	type: CodeableConcept [0..*]
10.1.1.1.	Reference to order e-document		indication: Order [0..1]
10.1.1.2.	Order number	Order	id: identifier [1]
10.1.1.3.	Order date and time	Order	date: dateTime [0..1]
10.1.1.4.	Order diagnosis	Condition	text : String [0..1]
10.1.1.5.	Order diagnosis code	Condition	code : String [0..1]
10.1.2.	Came without order (tag)		
10.2.	**Study description:**		
10.2.1.	Study (medical image) report number	DocumentReference	masterIdentifier: String [1]
10.2.2.	Study UID	ImagingStudy	uid: String [1]
10.2.3.	Study date and time	ImagingStudy	dateTime: dateTime [1]
10.2.4.	Study title	ImagingStudy	description: String [0..1]
10.2.5.	Study ACHI code	DiagnosticReport	name: codeableConcept [1]
10.2.6.	Patient not identified (tag)	Patient	identifier : codeableConcept [1]
10.2.7.	Attached file(s) (YES / NO):	List	entry: Image [0..*]
10.2.7.1.	File number	List	entry: Image [0..*]
10.3.	Study (medical image) description	DiagnosticReport	description: String [1]
10.4.	Conclusion	DiagnosticReport	conclusion: String [1]
10.5.	**Main diagnosis:**		
10.5.1.	TLK-10-AM code	Condition	code: CoadeableConcept [1]
10.5.2.	Title	Condition	display: String [1]
10.5.3.	Description	Condition	notes: String [0..1]
10.6.	Diagnosis 1		
10.7.	Diagnosis 2		
10.8.	**Ionizing radiation details:**		
10.8.1.	Device serial number	Observation	valueString: String [0..1]
10.8.2.	Dose	Observation	valueQuantity: Quantity [0..1]
10.8.3.	Unit of measure	Observation	valueQuantity: String [0..1]
10.9.	**Related studies:**		
10.9.1.	Title	ImagingStudy	description: text [1]
10.9.2.	Related study number	ImagingStudy	uid : String [0..1]

2.3.2. Used technologies

49. Orace EE.
50. Java.
51. Angular.
52. TypeScript.
53. RabbitMQ.
54. Flutter.
55. CentOS, Red Hat Fuse.
56. Power BI.
57. WildFly.
58. DCM4CHE.

[1] https://www.esveikata.lt/espbi-specifikacija

2.4. System file structure

59. MedVAIS file storage is ensured by two identical storage systems, which include:

59.1 Xcellis MDC – creates unified file system and ensures its high availability. Furthermore, ensures copying of file system data without additional user intervention.

59.2 Quantum QXS424 – high performance storage for file system metadata.

59.3 Bull Optima3700 – file storage.

59.4 Quantum QXS584 – file storage.

59.5 Quantum AEL500 – tape storage. Xcellis MDC can transfer (and restore) data form file storage automatically according to chosen policy.

59.6 Xcellis Workflow Extender – component responsible for replication between storages.

59.7 Quantum QXS584 together with Bull Optima 3700 creates medical image storage, where currently 1,4 Pb of data is stored.

3. DESCRIPTION OF THE DESIRED STATE OF THE SOLUTION

60. The aim is to modernize and implement the System, which would realize the following new functions:

60.1. **Access to medical images** – functionality that allows a healthcare professional to access and retrieve patients' medical images and their reports from different institutions that have submitted data to MedVAIS:

60.1.1. Possibility to request a list of patient studies using DICOM protocol;

60.1.2. Possibility to retrieve medical images according to the provided list using DICOM DIMSE services;

60.1.3. Possibility to retrieve medical images via DICOMweb services;

60.1.4. MedVAIS by using ESPBI IS user access rights mechanism can verify whether the PHCI and a specific physician have the right to access patient data.

60.2. **Medical image viewer** – a tool for viewing medical images (DICOM and non-DICOM), the availability of which is controlled by the user role. The functionality must be adapted to the user's work in the HIS environment and eHealth portals and must not require any installation actions on the user's computer.

60.3. **The possibility of transferring files in a non-DICOM format** – functionality that allows MedVAIS to receive and store non-DICOM files, with the aim of opening them in the same tool for viewing medical images and the ability to share via DICOM standard protocols between institutions. The functionality must be adapted to the user's work in the HIS environment and eHealth portals.

60.4. **Data registry and storage management** – MedVAIS must have data registry and storage management functionality that allows:

60.4.1. Migrate data from current PACS to new system.

60.4.2. Migrate data within existing infrastructure in cases where it is necessary to update its components.

60.5. **Enabling hybrid model** – after implementation of services described in this document, MedVAIS will perform the functions of the central registry and repository. However, the modernized system must also ensure the possibility to adapt a hybrid data storage model in Lithuania in the future:

60.5.1. In the case of hybrid data model, the function of medical image repositories would be performed not only by MedVAIS, but also by PHCI, which has the necessary infrastructure.

60.5.2. MedVAIS would perform the functions of the main register and one of the repositories of medical images.
60.5.3. In the case of a hybrid model, PHCI could choose to provide a medical image to MedVAIS for storage or provide information about the medical image with included link for retrieval to other PHCI.
60.5.4. PHCI would download a study from MedVAIS by querying MedVAIS or receive a link from the PHCI where the study is stored.
60.6. **Anonymization functionality** – modernized MedVAIS must be able to anonymize medical images (metadata and burned into pixel data) for secondary use.
60.7. **Data lifecycle management functionality** – updated MedVAIS system must be able to apply life-cycle management rules for medical images, other files in DICOM and non-DICOM format, which determine the use of storage memory spaces. It must be possible to manage the storage of data in different memory spaces based on events related to patient data and other (e.g. recorded visit).

The functionalities to be implemented are reflected in the scheme summarizing the protocols and components of the system (see Figure 6):

- VNA – data management between storage and memory units, ensuring intake and transfer of data regardless of the data provider's initial and preferred formats (vendor neutral metadata and binary files).
- DICOM server – implementation of DICOM standard protocols (DIMSE and DICOMWeb) for data transfer and access to the viewer, as well as metadata management.
- EHR – interface between medical image data and electronic health history registry and user components that directly use DICOM protocols (WADO-RS – transfer of medical images, STOW-RS – storage of medical images, DIMSE – data exchange between the system and image generating devices and other applications or systems that support DIMSE protocols).
- Storage options, Database layer and network components will be detailed during the implementation of the project.

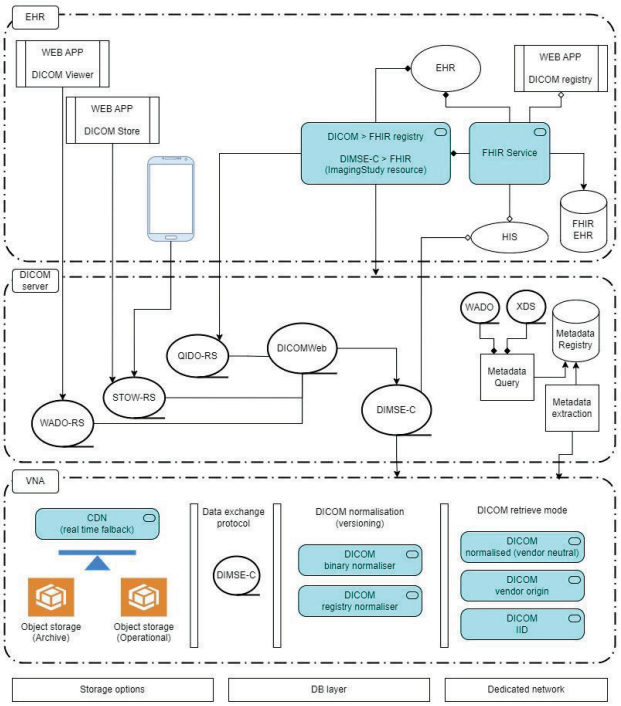


Figure 6. Diagram of the expected architectural components

4. DESCRIPTION OF FUNCTIONAL REQUIREMENTS

61. This section contains functional requirements that the Service provider will have to clarify and agree with the representatives of the Contracting Authority (hereinafter referred to as the Contracting Authority, Centre of Registers, RC) during detailed analysis and design phases. If necessary, the functional requirements may be adjusted, but only after agreeing and approving the changes with the Buyer. During the acceptance testing, the Provider will be required to demonstrate all of the following functional requirements.

4.1. General requirements

Requirement No.	Description
BR_1.	The Service provider shall follow the requirements of this Technical Specification and the Annexes to the Specification in developing all the functionality.
BR_2.	During development, all the functionalities currently available in the ESPBI IS must be maintained and not damaged.
BR_3.	The Service provider will have to cooperate with service providers of the parallel ESPBI IS modernization activities.
BR_4.	During the implementation of the project, following parts of the ESPBI IS must be strictly taken into account: 1. Used technologies. 2. Standard software used. 3. Data model architecture. 4. Architecture of servers, computer network and devices used in it. 5. Internal and external integrations and data flows. 6. Data classifications used. 7. User Identity and Access Rights Model. 8. Automated business processes.
BR_5.	MedVAIS functions must be developed as an integral part of ESPBI IS, using existing ESPBI IS tools for the provision of health care services and creating missing ones.
BR_6.	The standard functions and components of the ESPBI IS must be reused during the realization, e.g.: 1. For the auditing of actions carried out in the subsystem. 2. For document management (creation, use of drafts, etc.). 3. For functions related to communication (sending notifications, providing reminders, etc.). 4. For calendar-related functions. 5. Data analysis and reporting. 6. For administration and other functions. The Service provider will have to provide requirements for changes to the standard components of the ESPBI IS, which will be necessary for the realization of the project and the business processes associated with it.

BR_7.	The data entry forms that are created must be constructed in such a way that the data entry is structured as much as possible.
BR_8.	When implementing the functional and non-functional requirements of the project, the ESPBI IS administration tools must be modified accordingly, which will allow for the proper administration of the created functionalities.
BR_9.	The data entry forms shall, as much as possible, be completed in an automated manner with data already stored in the ESPBI IS or other IS and registers accessible through integration interfaces. The Service provider must, during the detailed analysis and design phases, determine and agree with the Contracting Authority which form data will be automatically filled in with the intended values.
BR_10.	Lists must include: 1. Pagination. 2. The lists must represent the number of entries in the list. After filtering the list, the number of records found must be represented. 3. It must be possible to filter and sort the list by the attributes that belong to that list. Exceptions may be made in agreement with the Contracting Authority.
BR_11.	All search / filtering functions, except for cases that will be agreed by the Provider during the detailed analysis and design phase, must be realized according to the following rules: 1. In the text search fields, a search by a fragment of a word or combination of numbers and a full word must be realized. 2. The search must be carried out according to Lithuanian letters and the Latin equivalents of the Lithuanian letters (for example, treating the letters "š" and "s" as one). 3. The search must be carried out by treating uppercase and lowercase letters as equivalent. 4. The search shall be carried out only in those components and datasets to which the user has access rights. 5. The search results must be presented in the form of a list. 6. After the search is done, the number of search results must be displayed.
BR_12.	Verification of the data entered into the data entry forms must be carried out in accordance with the validation rules established for forms during detailed analysis and design: 1. Mandatory data must be checked. 2. The format of the data (date, number, text or other established rules) must be checked. 3. The extensions and file size of the attached files must be checked. 4. A logical check must be carried out between the elements of the form - the selection (input) of one element of the form must be able to enable / disable other elements of the form.
BR_13.	For all functions described in this technical specification, during which data or documents are created, the functions of editing, removing or undoing those data or documents must be realized, which must be aligned with the business logic.

BR_14.	The rules for the management of datasets implemented or changed during the project must be the same as for the entire ESPBI IS.
BR_15.	The forms implemented during the project must comply with all the general requirements for ESPBI IS forms and be realized on a unified basis.
BR_16.	Access to functionality and data availability must be managed through a current ESPBI IS access control management.
BR_17.	The rules for signing document sets implemented during the project must be the same as ESPBI IS.
BR_18.	Users must be able to connect from any compatible device (e.g. computer, smartphone, tablet).
BR_19.	During the detailed analysis and design, the Service provider shall coordinate with the Contracting Authority the rights of the authorized, substitute specialist, patient representative, special users within the scope of the newly realized functions and supplement or create the necessary classifications.
BR_20.	Users must be able to set the notification option in their personal account settings according to their role. This functionality exists in ESPBI IS, but needs to be adapted to the new notifications that arise in the scope of the project.
BR_21.	The data of the common registers (classifications) in the System must be entered once, i.e. the data of any register cannot be duplicated.
BR_22.	During the development of the System, the Service provider must assess the requirements of the GDPR, design the data model of the System and implement solutions for the implementation of data subjects' rights in order to enable the rights of data subjects whose data are processed by means of the System to be implemented.
BR_23.	Information for users about the System and the processing of personal data carried out in it, the rights of data subjects and their implementation must be prepared.
BR_24.	During development, the System must be configured in such a way that by default the system parameters ensure the highest level of protection of personal data (privacy by default).

4.2. Functional requirements

Functional requirements related to medical image access:

Requirement No.	Description
FR_1.	It must be possible to request a list of medical images using the DICOM protocol (C-FIND, QIDO-RS).
FR_2.	It must be possible to download medical images according to the provided list using the DICOM protocol (C-MOVE, WADO-RS).
FR_3.	MedVAIS must be able to check whether it has a medical image in its repository according to the specified parameters of the query and provide an indication(s) of its state.
FR_4.	MedVAIS must be able to verify, using the current ESPBI IS access control management, whether the PHCI and the specific Specialist who made the request have the permissions of access to the Patient's EHR.

FR_5.	ESPBI IS must be able to send a message to PHCI HIS via the integration interface indicating the reason(s) for the failure to respond to the Request in the cases provided (but not limited to): when access to the Patient's EHR is not allowed, MedVAIS does not have requested medical image and in other cases agreed at the stage of detailed Analysis.
FR_6.	MedVAIS must be able to select all the studies of the patient from the DICOM database and form a list of studies according to the parameters provided in the request (DICOM DIMSE and DICOMweb).
FR_7.	MedVAIS must be able to transmit the medical image data specified in the request received from PHCI HIS and send it to the PACS used by the PHCI, depending on whether original, vendor neutral or other data is requested and could be provided via WADO-RS protocol.
FR_8.	MedVAIS Administrator must be provided with the access to service operation and usage logs and means to analyze it. The solutions and measures proposed by the Service provider must be agreed with the Contracting Authority at the analysis stage.
FR_9.	A multiparametric search function for information related to the operation and use of functionality in IS system logs must be created. The solutions and measures proposed by the provider must be coordinated with the Contracting Authority. The Service provider must take into account the suggestions of the Contracting Authority.
FR_10.	The Administrator of MedVAIS must be able collect and display the necessary statistical information related to the operation and use of the Functionality in the Administrator's environment. The solutions and tools proposed by the provider and the sample of statistical information must be aligned with the Contracting Authority. The Service provider must take into account the suggestions of the Contracting Authority.

Functional requirements related to medical image viewer:

Requirement No.	Description
FR_11.	Viewer must be accessible via web browser.
FR_12.	The component must identify users and authorize user permisions during a medical image review, according to the current ESPBI IS access control management.
FR_13.	Component user interface language must be changeable between Lithuanian and English languages.
FR_14.	The following functions for viewing DICOM files must be realized in the viewer, but not limited to them: 1. zooming in/out. 2. image inversion. 3. image rotation. 1. density measurement. 4. image window width / level parameter change. 5. change of image scale. 6. angle measurement.

	7. cross-section display.
FR_15.	Viewer must have the ability to display DICOM standard video (supported format types e.g. MPEG-2, MPEG-4, AVC/H.264, MP4 and others supported by the DICOM standard).
FR_16.	It must be possible to view non-DICOM format files with the viewer for which (JPEG, GIF, PNG, TIFF, PDF and other formats) the support is described in the DICOM standard and its annexes.
FR_17.	Viewer must be able to display DICOM file metadata.

Functional requirements related to the transfer of non-DICOM format files:

Requirement No.	Description
FR_18.	MedVAIS must be able to receive various types of multimedia files in a non-DICOM format that store the data of images and video, including in PDF format (examples of file types, but not limited to: JPG, PNG, BMP, TIFF, PDF, MOV, MPEG, MPG, AVI, MP4, WMV, HEIC), transforming them into a DICOM format both through an integrated interface and through a specialist portal.
FR_19.	When providing files in a non-DICOM format, it must be possible to submit data for the creation of DICOM metadata. It must be possible to provide metadata both through the PHCI integration interface (Web Service) and the specialist's portal. General rules of data validation must be prepared by the Service provider and agreed with the Contracting Authority.
FR_20.	When transferring a file in a non-DICOM format, it must be possible to select the DICOM modality attribute that will be applied to the file.
FR_21.	It must be possible to transfer non-DICOM files (original and converted to DICOM) using DICOM protocols after non-DICOM file is sent to MedVAIS.
FR_22.	It must be possible to view DICOM files, created from non-DICOM media via DICOM viewer after non-DICOM media is sent to MedVAIS.
FR_23.	Validation rules according to set criteria (e.g. person identification code is not provided) must be applied for non-DICOM file upload. Error messages must be provided if file doesn't meet the requirements.
FR_24.	Limitations (e.g. file format, size) non-DICOM file upload must be applied together with the accompanying error message. Both of which agreed in analysis stage.

Functional requirements related to the data register and storage management tool (hereinafter referred to as the "Tool"):

Requirement No.	Description
FR_25.	The tool must be able to flexibly configure the data migration/transfer work performed taking into account: job queue management, selection of initial data, hash algorithm selection (e.g. crc32, md5, sha256), selection of the planned data path structure template according to the source and other criteria (possibility to apply parameters for input and output path dependencies). The

	solutions and measures proposed by the Service provider must be coordinated with the Contracting Authority.
FR_26.	It must be possible to access and manage the data migration tool through the MEDVAIS Administrator portal.
FR_27.	Tool access management must be enabled for MEDVAIS administrators and users by applying the access control mechanism used in the project scope.
FR_28.	The tool must display status of the tasks in the migration process (including user who created the task, date and time of creation, start of execution, predicted end, and other relevant fields) and the task log.

Functional requirements related to the data anonymization:

Requirement No.	Description
FR_29.	The anonymization functionality must have an API for the transfer of anonymized medical images to other information systems for scientific and statistical purposes.
FR_30.	The anonymization of files is carried out by ensuring the traceability of the original file in the MedVAIS, i.e. MedVAIS maintains an encrypted anonymized and original file link, accessible based on the user permissions.
FR_31.	It must be possible to specify anonymization attributes for each anonymization task in the administrator portal.
FR_32.	It must be possible to manage the functionality of anonymization in terms of work queues and scheduled tasks.
FR_33.	It must be possible to manage the access rights of the anonymization functionality to the users of the administrator portal.
FR_34.	It must be possible to anonymize in a configurable way for a sensitive data embedded in both: metadata and images (burned into pixel data).
FR_35.	It must be possible to configure a minimum set of anonymized data that is set despite of other configurations and be always added by default in case of anonymization.
FR_36.	It must be possible to manage data to be anonymized by taking into account the expression of the will of individuals (patients).

Functional requirements related to the data lifecycle management:

Requirement No.	Description
FR_37.	It must be possible in the updated MedVAIS Administrator to apply lifecycle management rules for medical images, other files in the DICOM and non-DICOM format, determining the use of storage memory spaces.
FR_38.	It must be possible to manage data storage criteria in different memory spaces based on events related to patient data and other events (e.g. recorded visit, patient logged in to the portal menu on medical images, etc.).
FR_39.	It must be possible to configure user permissions for changing and viewing the data lifecycle configuration in the role management window.

5. NON-FUNCTIONAL REQUIREMENTS

5.1. Criteria for the implementation of non-functional requirements

Requirement No.	Description
NFR_1.	The Service provider must realize all the requirements of the specification.
NFR_2.	The terms "must be / have / ensure / allow / comply", "must be able to", "must be available" used in this document are equivalent and imply that the Service provider must develop and implement (or provide and install) the appropriate functionality and provide the relevant services. The functionality that is specified in the future time ("will", " will allow", "will cover") indicates the state to be implemented and implies that the Service provider must create and implement (or provide and install) the appropriate functionality.
NFR_3.	The Service provider or Contracting Authority may propose an alternative way of implementing a separate specification requirement or a change in the implementation of the requirement to an equivalent functionality that would not in any way adversely affect the purpose, objectives and final results of the Procurement and would not contradict the requirements of the procurement legislation. Every alternative or requirement-changing functionality offered must be agreed with the Contracting Authority. In the case of changing the requirement to equivalent functionality, the Service provider will have to provide a written justification, which includes a description of the impact and criticality of the change, justifying that the change does not affect the entire functionality of the System. An assessment of the exchanged functionality according to the time costs must also be carried out (the time spent on the realization of the exchanged functionality is detailed and the time spent on the realization of the new functionality is presented). The implementation of the alternative requirements of the specification must be subject to the change management procedure defined in the Services Regulation.
NFR_4.	The Service provider may offer alternative methods of architectural realization that would ensure equivalent or better system speed, availability, scalability, interoperability, support, security and convenience. Each proposal must be evaluated and approved by the Contracting Authority.
NFR_5.	All created services, applications must be placed in containerized environments and transferred to the Contracting Authority for CI/CD installation processes in Docker format.

5.2. Requirements for the System architecture

Requirement No.	Description
NFR_6.	The realization of the system must be based on a multi-layered architecture that would allow the System to be expanded and adapted to changing needs. The system architecture must be at least 4 layers and be able to be integrated at the levels of individual layers:

	1. Presentation Layer – must ensure the user's interaction with the information system and that the information is presented to the user. 2. Application Layer – must ensure that business processes and rules are applied to the information system's operational logic. 3. Integration Layer – must ensure the exchange of the necessary data both between the internal components of the System, where it will be relevant, and with external information systems. 4. Data Layer – must ensure the collection, processing and presentation of the data necessary for the operation of the information system.
NFR_7.	The system must be implemented according to the principles of Service-Oriented Architecture (SOA), maintaining as much independence as possible between the components that make up the system.
NFR_8.	Throughout the project, DICOM standard must be followed to include all the necessary technological mechanisms supported by the standard.
NFR_9.	The system must realize the possibility of providing information according to ATNA (Audit Trail and Node Authentication) as needed, ensuring that all system and its component actions and attributes associated with them are logged (included but not limited to: stack trace, service trace, audit trail and logging of other actions).
NFR_10.	The design of the system and its components must take into account the Single Source of Truth (SSOT) principle at the Data Level.
NFR_11.	Data layer must be realized by OS file system, databases and data repository or storage forms. In the data layer different data sets must be integrated into a single unified data exchange subsystem with components of business logic layer.
NFR_12.	The system functions implemented in the project shall have a fault tolerance and handling mechanism, load management and high system availability management capabilities through horizontal scaling.
NFR_13.	The system architecture must be adapted to enable the hybrid data model despite the fact that within the scope of this project such a model will not be realized.
NFR_14.	Architectural components must be stable and widely used in practice. The Service provider may not offer to use versions of software components that are in the testing phase, marked with "beta" or other means of indicating this.
NFR_15.	Architectural principles of design are presented in Figure 6. and the solution provided by the Service provider must maintain the data exchange protocols used by the DICOM standard (e.g. WADO-RS, STOW-RS, DIMSE) for the applicable functions.

5.3. Requirements for medical image viewer

Requirement No.	Description
NFR_16.	The component must work in the following browsers: • Microsoft Edge, from 128 ver. • Mozilla Firefox, from 128 ver. • Google Chrome, from 128 ver. • Safari, from 18 ver.

	The component must not require the installation of any additional software or plugins in the web browser.
NFR_17.	The component must fully integrate with ESPBI IS and with other MedVAIS components and must act as an integrated ESPBI IS e. Health portal component.
NFR_18.	The component must support Secure Data Transfer (SSL).
NFR_19.	The component must be certified as complying with the EU Medical Device Regulation (EU 2017/745) and bear the CE marking.
NFR_20.	The Service provider must provide in his tender a URL link of the website where the Contracting Authority can evaluate the viewer in accordance with the requirements of the technical specification.
NFR_21.	The viewing tool must be implemented according to the server-client principle, when image processing (e.g. preparation of medical images of different quality) must be carried out on the server side and rendered view is brought out to the client's side utilizing the capabilities of WADO-RS protocol. Due to the provision of speed, certain operations such as zooming can be carried out on the client's side, the list of such parameters is agreed at the stage of detailed analysis.
NFR_22.	The Viewer API must be able to change the viewer software (service) without changing the architecture of MedVAIS and its other components, but by changing the configuration parameters (e.g., in the administrator's space, indicating the URL or IP address of another service).
NFR_23.	The viewer must support at least all file formats described in the DICOM standard and its annexes.

5.4. Requirements related to the data register and storage management tool (hereinafter referred to as the "Tool"):

Requirement No.	Description
NFR_24.	When designing the operation of the Tool, it must be taken into account that the Tool must be able to manage the register of stored medical images and medical images at the DB and file storage levels in such a way as to ensure the availability of the transferred data to users in accordance with paragraph 5.6 of the non-functional requirements.
NFR_25.	When designing the operation of the Tool, the alignment of the Tool with the VNA must be taken into account.
NFR_26.	The tool must be designed and compatible with management of hybrid data storage model.

5.5. Requirements for technology

Requirement No.	Description
NFR_27.	The realization of the project must be based on generally accepted technological and operational standards (e.g. SOA, OSGi, SSL, etc.)
NFR_28.	In the presence of several possible interpretations of a standard or requirement, the principle of best practice must be followed.
NFR_29.	All functional components being developed must support the Unicode (UTF – 8) standard.

NFR_30.	For the realization of the project, the roadmap and lifetime of the technologies used must be taken into account and deprecated versions must not be used. The end-of-life date of the published versions must be at least 36 months after the implementation of the project. The exceptions shall be agreed with the Contracting Authority.
NFR_31.	New user interfaces must use Angular, React Native or equivalent technologies and technologies such as JavaScript, TypeScript and others must be used for modernized functionalities of the existing user interface.
NFR_32.	System must be based on Java or equivalent technologies.
NFR_33.	Postgres or equivalent technologies must be used for newly developed databases, existing databases and in cases where it is necessary, Oracle must be used.
NFR_34.	Technologies such as RabbitMQ, Nginx or equivalent must additionally be used to realize the project.

5.6. Requirements for system availability

Requirement No.	Description
NFR_35.	The architecture of the system must be adapted to maintain the availability of the System throughout the year, 24 hours a day and 7 days a week - at least 99.7 percent. Inactivity of the System infrastructure and scheduled work during which the System is down are not included in the availability percentage.
NFR_36.	The architectural solution must ensure the high availability (HA) of the System, which must be realized at the service level, at the integration level and at the data level.
NFR_37.	The System architecture and/or infrastructure proposed by the Service provider shall ensure the principle of interchangeability, i.e. in the event of failures of one or more components, the System shall continue to work with existing resources.
NFR_38.	It must be possible to work with the System while other works are being carried out, for example, the actions of the batch tasks performed, registrations, user actions must not block the actions of another user and must not affect the speed of the System, etc.
NFR_39.	High availability solutions must work automatically (in case of incidents). Human engagement may only be required to restore the system's performance to the state it was in before the incident.
NFR_40.	The high availability solution must be described in a detailed analysis and design document and approved by the Contracting Authority.

5.7. Requirements for scalability

Requirement No.	Description
NFR_41.	MedVAIS and its components must be the property of the Contracting Authority, except for the personal moral rights to the results of intellectual activity. At the end of the project, the Contracting Authority must be able to independently develop and adapt the functionality of MedVAIS and its

	components to new emerging needs, without additional licenses, fees or the intervention of third parties.
NFR_42.	The architecture shall support the expansion of the System's capacity by adding additional hardware or virtual infrastructure.
NFR_43.	Architecture must be designed on the basis of multi-level architecture, creating opportunities for its development at the level of individual layers.
NFR_44.	MedVAIS performance must be easily expanded by adding additional technical resources and hardware, without changing the code of the software. The capacity building of the technical equipment shall be carried out without suspending, as much as possible, the operation of the ESPBI IS.
NFR_45.	MEDVAIS must include measures to ensure that changes and/or configurations made at the database level are maintained when performing a change and/or update of the System and/or its individual components.
NFR_46.	Modification, improvement and correction of errors in the software cannot affect the integrity of previously entered data.
NFR_47.	The System must be implemented in such a way that no additional work should be performed when switching to a higher version of the System (changing/supplementing the functionality of the System) and/or changing the database (except for those recommended by the System manufacturer as standard when switching from one version of the System to another).
NFR_48.	When making a change and/or update in the system, there must be functionality that ensures that: 1. All stored data will be transferred to the new database structure. 2. The integrity of the data will be maintained. 3. No stored data will be lost. 4. The functionality implemented in the System will not be disrupted.

5.8. Requirements for the creation and restoration of backup copies

Requirement No.	Description
NFR_49.	The project must be realized in such a way that when making updates related to architectural components and / or changing the database, it is possible to carry out migration of all data without additional services and licenses for rent.
NFR_50.	When preparing a backup copy or archive, transactions carried out in the System must not be lost and data processed, i.e. before the preparation of the backup copy or archive, all ongoing transactions must be completed and the entered data stored.
NFR_51.	During the procedures for the backup of data, the requirements for system performance must be met.

5.9. Requirements for system monitoring

Requirement No.	Description
NFR_52.	The Service provider must ensure the necessary conditions and carry out the necessary work (such as preparing and describing the integration monitoring

	and control points required for monitoring, etc.) so that the contracting authority's specialists can connect the desired components to the monitoring software used (e.g. Zabbix, OpenTelemetry). All monitoring points shall be linked to the tools used by the Contracting Authority.
NFR_53.	It must be possible to monitor the performance indicators of the system and its individual components using WEB tools (active users, memory utilization, processor load and other important indicators) and receive messages in case of malfunctioning of components or when indicators reach critical values. It must be ensured that the contracting authority's specialists are informed to respond in a timely manner to possible disturbances before they occur.
NFR_54.	All services created or replaced during the project must support a centralized service tracing mechanism that ensures the monitoring of requests and operations throughout their execution chain. Tracking data must be generated and transmitted using Trace ID and Span ID, which are compatible with the tracking tool of choice (e.g. OpenTelemetry, Jaeger, etc.).
NFR_55.	Solutions for monitoring and early warning of the operation of MedVAIS and its components shall be implemented. It must be possible to monitor the performance of MedVAIS and its components, network, server performance and other relevant indicators, such as: 1. the number of users logged in at the same time. 2. CPU and memory load. 3. network bandwidth. 4. the average duration of the session. 5. the time it takes for the system to present the image to the client (applies to the viewer). The above-mentioned indicators are exemplary and not final. The Service provider will have to distinguish critical and other parameters (up to 10 indicators for each of the types of components). All monitoring points where these and other parameters are checked will have to be proposed by the Service provider, agreed with the Contracting Authority and described during the detailed analysis and design phase.

5.10. Requirements for a data model

Requirement No.	Description
NFR_56.	The Service provider during development for data management must apply "Once only" principle to keep as little data as possible, while relying on queries to primary sources.
NFR_57.	Pre-aggregated and lookup data tables must be used to extract additional information to reduce the load on the processing of the main data and ensure the optimization of queries.
NFR_58.	When designing the realization of this project, the list of structured data must be constantly updated and agreed with the Contracting Authority.
NFR_59.	All the operational data of this project named in the technical specification must be realized in the project data model. The provider must realize all the

	data entities (along with attributes and interfaces) that are necessary to create the functions specified in the specification.
NFR_60.	When designing the data model for this project, the medical imaging registry must be compatible with the architectural principles of the hybrid model.
NFR_61.	The Service provider must migrate the existing data registry records (Oracle DB data) and medical image storage (StorNext disk storage) data to the modernized system according to the agreed migration work plan.

5.11. Requirements for system administration

Requirement No.	Description
NFR_62.	The System Administrator must be able to create login data (login and password) for System users, enter the name and surname of the System user, e-mail address.
NFR_63.	System administrator must be able to manage user permissions via access control management
NFR_64.	The System shall not limit the number of registered users of the System.
NFR_65.	The System Administrator shall be able to view the Audit Log of user actions, which will record all the actions of users, the systematic error messages they receive, as well as what data and how it has been changed. The date, time, username of the action, the IP address of the network of Internet access users or the IP and MAC addresses of users of the internal network must be recorded.
NFR_66.	It must be possible for users to see the level of their access rights. This visibility must be controlled by the System Administrator.

5.12. Requirements for performance and speed

Requirement No.	Description
NFR_67.	New project features must meet performance requirements: 1. Opening a detailed window (with all the desired objects) should take no more than 2 seconds. 2. The data saving operation after a change must not take more than 1 second. 3. Responses from the web services involved in the data exchange must be made within 2 seconds or less. 4. The presentation of the menu list (selection of System Functions) to users must not exceed 1 second. 5. Navigation between the different windows of the System user interface (both opening a new window and replacing a window) must take no more than 2 seconds (except when a report is generated). 6. Navigation between different data entry fields must take no more than 2 seconds (except when a report is generated). 7. It must take no more than 1 second to return the values in the list (for the values of a specific classifier).

	8. Searching the system for data, displaying a finite search result for up to 5 (five) seconds, except for complex, complicated queries. 9. Automatic (batch, background) tasks (for bulk processing) - The system must process at least 100 objects in 1 second (all intermediate data processing, data manipulation, writing to intermediate tables, etc. must be done at the same time). During the project, functions that are not covered by the durations provided for in this requirement may be coordinated with the Contracting Authority and specific complex cases (e.g., during which information aggregation is carried out) for which other speeds are applied may be agreed. These exceptional cases may be applied only with the approval of the Contracting Authority. Speed requirements do not include the Service provider's infrastructure's internet connection.
NFR_68.	The Service provider shall provide the Contracting Authority with a performance testing environment.
NFR_69.	The Service provider will be required to carry out load tolerance testing of the system and submit a report to the Contracting Authority. The image viewer must be tested at up to 2 times the specification load without loss of performance stability, with only degradation of performance possible. The Service provider undertakes to resolve any deficiencies found during the testing if the test results do not meet all the specified performance and speed requirements. Load testing scenarios: 1. User login tests. Simulate a large number of users while logging into the platform at the same time. 2. Image viewing tests. Simulate a large number of users who view different medical images at the same time. 3. Load tests. To test how the system works with a large number of concurrent users - from a few to tens of thousands. 4. Reliability and stability tests. Simulate long-term image viewing sessions with hours of a full working day. 5. Determination of the limits of available resources based on the ranges of the load level. Simulate scenarios where resource limits are reached (CPU, RAM, network bandwidth, etc.).
NFR_70.	Auditing of functions and user actions, that exceed the established performance requirements described above, must be realized. The audit record must contain sufficient data to determine which component and/or function of the project does not meet or increases the risk of not meeting the performance requirements in certain circumstances.
NFR_71.	Longer lasting processes (functions performed) must be indicated, and the user interface must clearly identify when ESPBI IS, MedVAIS and their components are working properly (e.g. sending a large-scale medical image).
NFR_72.	The execution of automated (background, batch, report) tasks must not affect the work of System users.
NFR_73.	The realization of the integration interfaces must ensure that the integration scenarios defined during the design process will occur within a reasonable time interval and do not in any way adversely affect the convenience and performance of the use of ESPBI IS.

5.13. Requirements for software and software licenses

Requirement No.	Description
NFR_74.	The system software must be installed on the server. No System components must be installed on the User's computer (workstation).
NFR_75.	All software that will be created within the scope of the Project, except for the personal moral rights to the results of intellectual activity, must be fully transferred to the Contracting Authority (all property rights, source codes and configurations transferred).
NFR_76.	The system must be designed in such a way that the data and business logic are stored in configurable repositories or external sources and not embedded directly in the code (not Hard Coded).
NFR_77.	The source code of the software developed during the project shall be provided to the Contracting Authority in the form of Docker images with standard compiler tools and compilation workflows and with the source code of the compilation scripts, and the developed code shall be stored in the Contracting Authority Git repository.
NFR_78.	The source code of the software developed/upgraded by the project shall be fully annotated and shall follow good practices for formatting, variable and function naming, including but not limited to the practice of using the name to understand the purpose of the code element and the practice of formatting the code so that the structure of the code is understood.
NFR_79.	The source code of the software code shall be subject to ISO/IEC 5055:2021 or equivalent standard(s), the actual scope of application of which shall take into account the technology used and shall be agreed with the Contracting Authority The service provider must prepare Unit tests and other parts agreed with the Contracting Authority that enable the CI/CD process through the use of best practices and automated testing (e.g., tools such as SonarQube or equivalent) for the quality management of the source code.
NFR_80.	Full, correct source texts must be transmitted to the Contracting Authority, from which, using standard and publicly available means, ready-to-use software is compiled, performing functions specific to it.
NFR_81.	If additional licensed software is to be used for the implementation of the project for the modernization of the subsystem, the licensing procedure for such license software must be of continuous validity (without any restrictions of validity in time and without any additional fees in order to expand or maintain the functionalities) so that the Contracting Authority does not have to purchase additional licenses or otherwise incur costs for the operation of the software. The installer must provide such software and licenses for all IS environments to be installed (testing, training and production environments).
NFR_82.	Each additional licensed software proposed for use must be aligned with the Contracting Authority.
NFR_83.	When offering additional licensed software, the cost of purchasing it and maintaining it for at least 3 years (calculated from the end of the testing phase) must be included in the offer price.

NFR_84.	The Service provider must compensate the Contracting Authority against any claims arising out of the use of copyrights, patents, licenses, or trademarks in connection with the use of the software developed, unless such infringement is due to the fault of the Contracting Authority.
NFR_85.	Software with compilation source code must be delivered in Docker container format, ensuring that all dependencies and components required for execution are included.
NFR_86.	The source code to be transmitted shall be provided only in electronic form and shall meet the following requirements: 1. The source code must be placed in the Contracting Authority's GIT environment before each installation and the installation packages prepared from there to the test and production environments. 2. The source texts must be transmitted to the Contracting Authority in the form of packages of files prepared for compilation, indicating the standard compilation tools, the compilation process and together with all the libraries necessary for compilation. 3. The source texts must contain detailed comments and comply with good practices in the formatting of the code, the naming of variables and functions, including, but not limited to, the practice of understanding the purpose of the code element by the name and the practice where the formatting of the code allows you to understand the structure of the code. 4. The source code must be 70 – 80 % covered by automatic tests (unit tests). Testing of all features, user interfaces, and integration must be ensured. 5. Full, correct source texts must be transmitted to the Contracting Authority, from which, using standard and publicly available means, ready-to-use software is compiled, performing functions specific to it. 6. A test of the source code for the acceptance testing must be developed by performing the compilation of the source texts in the Contracting Authority's environment and functional testing of the version obtained during compilation. 7. After the Service provider makes changes to the software during the warranty, the source code will have to be updated and provided in accordance with the conditions set out in the above clauses.
NFR_87.	The compilation, configuration and deployment of the project shall be carried out from software code repositories located within the Contracting Authority's infrastructure using automated Continuous Integration tools. In cases where such tools are not available, the Service provider shall install them in the infrastructure of the Contracting Authority.
NFR_88.	The Service provider must provide and include in the price of the offer all the necessary standard and non-standard software, if necessary to ensure functionality and efficient work (meeting performance requirements).
NFR_89.	If necessary, the Service provider shall perform hardware configurations. It must be carried out without the need for additional funds from the Contracting Authority.
NFR_90.	The realization of changes in the functionality and functionality of the new software must not require the purchase of additional technical and licensed standard and non-standard software for the Contracting Authority.

5.14. Requirements for integrations

Requirement No.	Description
NFR_91.	The system shall implement the preliminary integration interfaces specified in the requirements of this document. Detailed integration interfaces will have to be agreed during the Project.
NFR_92.	The system must implement the necessary integration endpoints agreed during the detailed analysis and design phase. The Service provider must clearly define and describe the specifics of the integration endpoints. Sample structure of the description: 1. Name of the endpoint. 2. Aim. 3. Description. 4. Data source (e.g. user actions, DB logs, API queries). 5. Data transfer mechanism (e.g. HTTP, REST API). 6. Protocol (e.g. HTTPS). 7. Data format (e.g. JSON, XML). 8. Detailed examples of the content of the data provided.
NFR_93.	The integration interfaces of the system must be realized using the application programming interface (API).
NFR_94.	The Service provider shall prepare and agree on a technical specification for the integration interface, i.e. the design documentation for the integration interface, on the basis of which the other parties will have to carry out the necessary development work on the information system for the required integration interface.
NFR_95.	Where possible, internal and external data exchanges relevant to the subsystem must be carried out using existing ESPBI IS tools.
NFR_96.	The Service provider shall ensure that the functioning of the integration interfaces already in place is not disrupted.
NFR_97.	Interfaces must provide clear error messages (for example, HTTP responses with codes: "400 Bad Request", "503 Service Unavailable").
NFR_98.	Interfaces must support a large number of users at once. A stress analysis will have to be carried out and its results provided to the Contracting Authority.

5.15. Requirements for user interface and ease of use

Requirement No.	Description
NFR_99.	The user interface shall be in line with the design trends prevailing at the time of purchase and in line with the contracting authority's identity (colors, fonts). Examples of the user interface can be presented in separate parts (UI and UX). The final decision shall be approved by the Contracting Authority from the models submitted.
NFR_100.	User interface error messages must be formulated in such a way that it is clear to the user what happened and what actions need to be taken next in order to continue working.

NFR_101.	All messages of the same type (errors, warning, etc.) must be presented in the same style (in the same place on the screen, in the same style, distinguished by the same colors).
NFR_102.	The user interface shall be tailored to the type of users and service recipients and access rights. Users shall only be presented with the functionality relevant to them and shall not be able to see functionality of the System that is not necessary or not permitted for their work.
NFR_103.	The user interface must be implemented in Lithuanian and English (Lithuanian as the default) and used in accordance with the general rules of the language. The supplier must coordinate the translations with the Contracting Authority during the detailed analysis and design phase.
NFR_104.	The data fields must be subject to logical validation at the field level (for example, a person's name cannot contain numbers) and at the group level of fields (for example, the start date of a search must be earlier than the end date of the search). Before saving the submitted data, a thorough logical check must be carried out (e.g. whether all the required fields are filled in).
NFR_105.	Data fields in data entry forms must be filled in automatically if the corresponding data is stored in the System database or integrated databases.
NFR_106.	The user interface must always show a full and interactive navigation path (Breadcrumbs).
NFR_107.	The user interface must adapt to screens of various sizes (Responsive design).
NFR_108.	It must be possible to provide contextual help for Complex functions or blocks of information.
NFR_109.	All functional components created or changed must correctly store, process and display information in Lithuanian and English with specific Lithuanian characters and rules.

5.16. Requirements for data archiving

Requirement No.	Description
NFR_110.	It must be possible to identify data or groups of data that can be archived and an automatic mechanism to ensure the archiving of this data must be implemented. The data archiving solution must be agreed with the Contracting Authority.
NFR_111.	The data must be transferred to the data archive according to the criteria agreed during the project analysis phase.

5.17. Requirements for the application of standards

Requirement No.	Description
NFR_112.	The MEDVAIS subsystem must be implemented in accordance with the ISO 12052:2017 standard.
NFR_113.	The MEDVAIS subsystem must be implemented in accordance with ISO 10781:2023 Electronic Health Record-System Functional Model, Release 2.1 or newer equivalent standard.

NFR_114.	ISO/IEC 5055:2021 or equivalent standard(s), the objectives of which are to define the quality of the source code of the software being developed and the automated verification of the quality of the source code. The scope of application of the selected standard is discussed in the light of the technologies used and is agreed with the Contracting Authority at the stage of detailed analysis.
NFR_115.	The user interface must meet the accessibility requirements of WCAG level 2.2.
NFR_116.	The user interface must comply with W3C HTML5 and CSS3 standards.
NFR_117.	The user interface must be developed in accordance with the requirements and recommendations of the LST EN ISO 9241 family of standards.
NFR_118.	In the analysis and design documents prepared by the Service provider, at least Unified Modeling Language (UML) version 2.0 or Business Process Model and Notation (BPMN) version 2.0 must be used for the design of business process diagrams, models, database diagrams, interface diagrams of software components and interface diagrams of other entities.
NFR_119.	The AES, equivalent or newer encryption standard must be used.
NFR_120.	The developed software must comply with international security standards LST ISO/IEC 27002, LST ISO/IEC 27001 or equivalent.
NFR_121.	The X.509 or later standard must be supported using digital certificates in interactions: system - system and system - user.
NFR_122.	To ensure the secure transmission of data transmitted over the Internet, the TLS (Transport Layer Security) protocol, version 1.2 or higher, must be used, both in communication between the system and the user, and, if necessary, between systems.

6. REQUIREMENT FOR SERVICE PROVISION

6.1. Requirement for workplace

Requirement No.	Description
PR-1.	In accordance with the established procedures, the Service Provider's employees participating in the execution of the Procurement Object (hereinafter referred to as the Supplier's specialists) will have access to the resources of the Contracting Authority (hereinafter referred to as access): 1. The provider's specialists will be given access to the Contracting Authority's applications: JIRA, CONFLUENCE. 2. The provider's specialists, application programmers will be granted access to the Contracting Authority's GIT repository for the management of the source code versions of the Procurement Object software, as well as to the servers for the execution of the Procurement Object in the Infrastructure Development Environment (DEV) (without granting administrative rights) and the necessary databases (DB) schemes. As needed, the Contracting Authority will provide secure remote access in the form of a dedicated virtual workstation (Virtual Desktop Infrastructure, hereinafter – VDI), through which the Provider's specialists will access the resources of the Contracting Authority necessary for the provision of the Services.

PR-2.	According to the need, the Contracting Authority will be able to provide the computer workstations of the Provider's specialists with secure remote VPN access to the dedicated resources necessary for the execution of the Procurement Object.
PR-3.	The supplier's specialists will not have access to the Contracting Authority's production data or production environments. All development, testing and maintenance work will be carried out in the Contracting Authority Development (DEV) and Testing (TEST) environments using anonymized or test data provided by the Contracting Authority.

6.2. Requirements for ordering services

Requirement No.	Description
PR-4.	The Service Provider may provide additional services, within the scope of which the Contracting Authority may order additional functionalities. Volume of development services – up to 300 hours.
PR-5.	Procedure for ordering additional functionality: 1. need for additional functionality is identified. 2. need shall be confirmed by the Contracting Authority. 3. The service provider prepares a proposal in which he describes the principles of realization of additional functionality, the term of realization and evaluates the number of hours required for realization (Annex x. order form). 4. After the Contracting Authority approves the offer, an additional functionality order is formed on the basis of the proposal, which is signed by the Contracting Authority and the Service Provider.
PR-6.	The requirements defined in this RPO and the solutions that elaborate on them cannot be considered as additional functionalities.
PR-7.	The approved services will be ordered by the Contracting Authority submitting tasks in JIRA – specific tasks are assigned to the Supplier's specialist(s) who have previously been granted access to the Contracting Authority's JIRA (see RPO PR-1).
PR-8.	The minimum 12-month warranty must apply to all additional services ordered.

6.3. Requirements for the implementation of the RPO

Requirement No.	Description
PR-9.	The Service provider is obliged to realize the requirements of the RPO.
PR-10.	The Service provider or the Contracting Authority may propose an alternative way of implementing a separate requirement of the RPO, or the exchange of the implementation of the requirement for equivalent functionality, which would not in any way adversely affect the purpose, objectives and final results of the Procurement, nor would it contradict the requirements of the legal acts governing procurement. Any proposed alternative or replacement functionality must be agreed with the Contracting Authority. In the case of changing the requirement

	to equivalent functionality, the Service provider will have to provide a written justification, which includes a description of the impact and criticality of the change, justifying that the change does not affect the entire functionality of the System. An assessment of the exchanged functionality according to the time costs must also be carried out (the time spent on the realization of the exchanged functionality is detailed and the time spent on the realization of the new functionality is presented). The implementation of the alternative requirements of the specification must be subject to the change management procedure defined in the Services Regulation. The Provider may offer alternative methods of architectural realization that would ensure equivalent or better system speed, high availability, scalability, interoperability, support, security and convenience. Each proposal must be evaluated and approved by the Contracting Authority.
PR-11.	The Service provider together with the proposal shall provide technical documentation and documentation of the proposed software confirming that the Service provider is the manufacturer of the proposed equipment or the official representative of the manufacturer and / or an authorized partner with the right to sell and install and / or configure the proposed equipment.
PR-12.	The Service provider, together with the Agreement, signs an agreement on the processing of personal data.
PR-13.	The Service provider shall ensure that the person who will carry out the implementation of the technical part of the Contract signs a Confidentiality Undertaking supplied by the Contracting Authority.
PR-14.	The Service provider must follow the versions of legal acts relevant during the performance of the Contract. The Service Provider is also bound by all newly adopted / amended legal acts during the performance of the Contract, if they are related to the implementation of the Contract. If the newly adopted / amended legal acts contradict the requirements described in the Technical Specification, the Service Provider shall implement the requirements in accordance with the versions of legal acts adopted / amended during the performance of the Contract.
PR-15.	Within 5 working days after the entry into force of the Agreement, the Service provider must hold an introductory meeting with the Centre of Registers and submit for coordination and present the Regulation on the Provision of Services (the main parts are indicated in Table 4).
PR-16.	The Service provider will have to communicate with the Contracting Authority during meetings, in writing and by e-mail, and to participate in the discussion of the documents being prepared with interested parties and to provide assistance in presenting and discussing the content of the documents submitted and to provide other consultations related to the preparation of the Specification to the Centre of Registers. The content of all meetings must be recorded in the manner specified in the Rules for the Provision of Services.
PR-17.	The Service provider is responsible for purchasing the necessary tools and hardware to perform the Services.
PR-18.	The specialists proposed by the Service provider must be able to communicate verbally and in writing in Lithuanian and English (at least at level C1 according to the Common European Framework for Reference for Languages). If the specialist does not speak Lithuanian or English, the requirement may be fulfilled

	by ensuring translation services during the performance of the Contract, which must be included in the price of the offer.

6.4. Requirements for service stages and software development iterations

Table 4. Stages of the implementation of services

Stage	Description of responsibilities	Results/requirements	Deadline
Initialization	Service provider: 1. Prepares Regulation on the provision of services, a detailed schedule of works and agrees with the Contracting Authority. Contracting Authority: 1. Provides the necessary information. 2. Provides comments and recommendations.	1. A Regulation on the provision of services has been prepared. The Service Provision Regulation specifies the objectives of the project, priorities, the scope and results of the stages, the interested parties, the schedule of execution of the work, the qualitative requirements, the risks and ways to manage them, the principles of communication, the criteria for the acceptance of responsibilities, intermediate and final results, the procedure for managing additional orders and other relevant information. 2. A detailed work schedule has been prepared, and milestones have been provided.	The results of the stage must be submitted and agreed with the Contracting Authority no later than within 10 working days from the date of entry into force of the Contract for the Provision of Services.
Detailed analysis	Service provider: 1. Conducts assessment of the AS-IS and TO-BE situation. 2. Prepares detailed analysis documentation. 3. Conducts other needed analysis Contracting Authority: 1. Provides the necessary information. 2. Provides comments and recommendations. 3. Approves the submitted results of the stage.	1. A detailed analysis document has been prepared, which analyzes and details the functional and non-functional requirements of the RPO and other needs expressed by the Contracting Authority, prepares user stories and use cases, which are presented according to the UML notation and detailed by describing the steps of execution of each use case (main course, alternative course, exclusive progress) and other restrictions. If necessary, IS users and their rights are described.	According to the agreed schedule of work.

Design	Service provider: 1. Performs design activities and prepares design documentation. 2. Prepares and aligns the technical specification for infrastructure requirements. 3. Analyses and prepares documentation describing the integration interfaces. 4. Aligns new integration links with data providers and recipients. 5. Develops specifications for the integration interfaces and coordinates them with the recipients and providers of the data and the Contracting Authority. 6. Updates and agrees with the Contracting Authority the technical description of the ESPBI IS. Contracting Authority: 1. Provides the necessary information. 2. Provides comments and recommendations. 3. Approves the submitted results of the stage.	1. Developed Design Document (the document contains: a description of the project architecture in terms of physical components and software components, the technologies used (their names, versions), an informative view (database structures, database interface diagrams, etc.), a functional image (functional units of the project, their functions, interrelationships, prototypes of the user interface), an integrative image (interfaces between internal and external systems, in relation to the system being developed), operational picture (system processes, algorithms, periodic system work, etc.), deployment view (distribution of software components in hardware), security solutions, high availability solutions, scalability solutions, etc.); 2. A technical specification of infrastructure requirements has been prepared (the document contains detailed requirements for technical and system software, which will be needed to ensure the proper functioning of the solution proposed by the Provider. At a minimum, the following must be provided: requirements for technical equipment; requirements for system software; analysis and requirements of the compatibility of the additional hardware and system software with the existing infrastructure of the Contracting Authority.) 3. Prepared document of technical architecture. 4. Logical DB model created. 5. Specifications for integration interfaces have been prepared. 6. A technical description (specification) has been prepared. 7. Developed primary guidelines for the user interface, which include: 7.1. user interface diagrams. 7.2. structure and design. 7.3. an initial prototype of the user interface has been prepared.	According to the agreed schedule of work.

Programming	Service provider: 1. Prepares plan for deployment to the test environment; 2. Carries out the necessary programming and configuration work (in its own development environment), implements functional and non-functional requirements; 3. Develops and submits a testing plan; 4. Performs unit testing, internal security testing, subsystem internal testing, interface testing with other systems; 5. Carries out demonstrations of the subsystem being developed, takes into account the comments made by the Contracting Authority; 6. Develops acceptance testing scenarios; 7. Prepares an internal testing report; 8. Revises detailed analysis and design documentation (if necessary). Contracting Authority and technical supervision (according to the competences): 1. Provides the necessary information; 2. Prepares production and testing environments on existing infrastructure; 3. Participates in subsystem demonstrations, provides feedback; 4. Reviews and evaluates the results of internal testing; 5. Provides comments and recommendations;	1. A plan for deployment into the test environment has been developed and agreed upon; 2. Prepared and agreed testing plan; 3. Prepared testing environment in the infrastructure of the Contracting Authority; 4. A demonstration of the subsystem being developed was carried out; 5. An internal testing report is provided describing the results of the internal security testing performed and the results of the internal testing (scope, execution methodology, types of testing, procedure, entry/exit criteria, testing environment), providing information on the areas of the subsystem that require additional attention during testing; 6. Software for prepared for deployment; 7. Detailed analysis and design documentation has been updated if needed.	According to the agreed schedule of work. The internal testing report must be submitted at least 5 working days before the start of the deployment phase of the testing environment. Demonstrations of the subsystem being developed must be carried out continuously, according to a separately agreed schedule.

Stage	Description of responsibilities	Results/requirements	Deadline
Deploying to a test environment	Service provider: 1. Prepares and submits the software suitable for installation in the Contracting Authority's testing environment. 2. Consults the Contracting Authority on deployment into the Contracting Authority's testing environment. 3. Prepares data loading scripts into the Contracting Authority's test environment; 4. Develops acceptance testing scenarios, testing methodology and plan. 5. Prepares instructions for users and administrators. Contracting Authority and technical supervision: 1. Reviews and evaluates the deployment plan. 2. Provides the necessary information. 3. Controls the testing environment. 4. Reviews and evaluates the testing plan. Contracting Authority: 1. Installs the submitted software into the Contracting Authority's testing environment; 2. Controls the testing environment. Data providers/recipients: 1. Reviews and evaluates the testing plan.	1. Prepared software for installation into the Contracting Authority's testing environment; 2. The software is installed in the Contracting Authority testing environment; 3. Test scenarios has been created; 4. Data for testing (in the form of SQL and / or other scripts) has been prepared; 5. A testing plan has been developed and agreed with the Contracting Authority and data providers/recipients; 6. Acceptance testing scenarios, testing methodology and plan has been prepared; 7. User guides and administrators' instructions ready.	Deployment must be completed by the beginning of the acceptance testing phase according to the agreed work schedule.

Stage	Description of responsibilities	Results/requirements	Deadline
Testing	<u>Service provider:</u> 1. Performs testing with data providers and recipients in the Contracting Authority's test environment; 2. Makes adjustments based on the comments made and corrects errors; 3. Creates all the technical documentation for the project; 4. Prepares a test report. <u>Contracting Authority and technical supervision:</u> 1. Provides the necessary information; 2. Record the errors detected by the Contracting Authority during the testing; 3. Carries out control over the elimination of problems identified during testing.	1. Integration Testing Report. The integration testing report must assess the defects identified during the integration testing, the method and status of their resolution; 2. All technical documentation has been created; 3. Analysis and design documents, installation instructions, project assembly and compilation instructions created; 4. Created instructions for users and administrators; 5. Prepared Error Elimination Reports.	The integration testing phase must be completed before the start of the introduction into the production environment according to the agreed work schedule.

Stage	Description of responsibilities	Results/requirements	Deadline
Acceptance testing	Service provider: 1. Develops user manuals and administrative instructions. 2. Adds new information to the ESPBI IS help system on the basis of developed and agreed user guides. 3. Conducts acceptance testing. 4. Eliminates recorded flaws (errors). 5. Makes the necessary adjustments based on the results of penetration and performance testing. 6. Prepares an acceptance testing report. 7. Prepares test scenarios. Contracting Authority: 1. Provides comments on the acceptance testing plan and testing scenarios; 2. Conducts acceptance testing according to the testing methodology and testing scenarios defined in the testing; 3. The selected independent Provider conducts security testing in accordance with the testing methodologies and testing scenarios defined in this technical specification; 4. Accepts software for trial operation.	1. Successfully completed acceptance testing. 2. The necessary changes have been made based on the results of penetration and performance testing. 3. User manuals and administrative instructions have been prepared. 4. Acceptance testing report has been prepared. 5. Accepted software for trial operation.	Acceptance testing shall be carried out prior to the start of the trial operation in accordance with the agreed work schedule.

Stage	Description of responsibilities	Results/requirements	Deadline
Deployment into the production environment	Service provider: 1. Provides a plan for deployment to the production environment; 2. Provides a plan for the start of trial operation; 3. Prepares and provides the software suitable for installation in the contracting authority's production environment; 4. Prepares data loading scripts into the contracting authority's production environment; 5. Prepares and aligns a pilot operation plan; 6. Revises the instructions of users and administrators. Contracting Authority: 1. Reviews and evaluates the deployment plan; 2. Provides the necessary information; 3. Leads the launch of new functionality; 4. Reviews and evaluates the pilot operation plan; 5. Depluys the provided software into the production environment; 6. Controls the production environment.	1. Software is prepared for deployment to the production environment; 2. The software is deployed to the production environment; 3. Prepared data for production operation (in the form of SQL and / or other scripts); 4. A plan for the start of the operation has been prepared; 5. Coordinated launch plan for new functionality with all data recipients/providers; 6. Performed the launch of a new functionality. Within a specified period of time, the system is ready for operation. 7. Installation documentation (including, but not limited to, detailed in section 6.4.4): 7.1. Deployment descriptions that must include: 7.1.1. Summary description of realized solutions. 7.1.2. Descriptions of data structures, attributes, data exchanges. 7.1.3. Description of technical realization (which includes the detailing of the requirements for the technical solution, the possibilities of expanding the System). 7.1.4. Other relevant information. 8. Source code and detailed project compilation instructions. 9. Deployment plan that includes: 9.1. Responsibilities of the people involved in deployment. 9.2. Description of deployment activities. 9.3. Schedule of deployment activities. 9.4. Deployment scheme.	Deployment can take place only after a successful acceptance testing. This stage of deployment must be completed within 1 (one) week after the end of the acceptance testing phase and completed by the start of the trial operation.

Stage	Description of responsibilities	Results/requirements	Deadline
Training (if necessary)	Service provider: 1. Prepares a training environment (if necessary); 2. Conducts training. Contracting Authority: 1. Ensures the participation of training participants in the trainings organized by the Service Provider. 2. Carries out training control.	1. Training documentation (including, but not limited to, detailed in section 6.4.6): 1.1. Training plan. 1.2. Guides for administrators and users. 1.3. Help Guide (electronic format). 1.4. Training materials (detailed requirements in section x). 1.5. Developed methodological recommendations for data providers and recipients. 2. Completed trainings for the agreed number of users. 3. Prepared training report.	According to the agreed schedule of work.
Pilot testing	Service provider: 1. Provides consultations during pilot operation; 2. Responds to defects detected during pilot operation; 3. Ensures expert advice to the Contracting Authority's staff and IT professionals; 4. Prepares a report on the pilot operation; 5. Ensures the integrity of system data. Contracting Authority and technical supervision: 1. Works with the prepared system; 2. Record errors detected during the pilot operation;	1. The errors found during the pilot operation have been eliminated. During the pilot operation, the Service provider must, in accordance with the agreed error elimination schedule, eliminate any defects in the functionality of the system recorded in the register of problems in the pilot operation; 2. Documentation for the pilot operation (including, but not limited to, detailed in section 6.4.7): 2.1. Pilot operation report. The report must include an assessment of the defects found during the pilot operation, the method and state of their resolution, and recommendations for further operation; 2.2. Register of problems during pilot operation.	According to the agreed schedule of work.

Stage	Description of responsibilities	Results/requirements	Deadline
Acceptance-transfer	Service provider: 1. Updates the technical documentation; 2. After the implementation of all services, provides a final report on the execution of the contract. Contracting Authority and technical supervision: 1. Accepts and approves the results prepared by the Service provider; 2. Signing of the transfer-acceptance act; 3. Provides comments and suggestions for improvement on the documentation provided by the Service provider.	1. Final report on the execution of the contract; 2. Transfer-acceptance act; 3. Prepared project documentation.	All services must be provided except for warranty.
Warranty	Service provider: 1. Prepares a regulation on warranty; 2. Provides warranty for the intended period. Contracting Authority: 1. Works with the prepared system; 2. Records errors detected during operation.	1. Document for the warranty procedure is prepared and agreed upon; Described in section 6.6 "Requirements for warranty".	The document of the warranty procedure must be submitted one month before the completion of the Project implementation.

6.4.1. Requirements for documentation and its coordination

Requirement No.	Description
PR-19.	All project documentation prepared by the Service provider must be prepared in Lithuanian in accordance with the rules of the common Lithuanian language (except for technical documents, where information may be provided in English), illustrated with diagrams, tables, graphs and other visual means, and the presented material is arranged in a clear, consistent and detailed manner.
PR-20.	Service provider's amended documents must be provided with visible changes (track changes function).
PR-21.	The documents agreed with the Contracting Authority shall (may) be amended during subsequent stages, provided that changes are made to the system being modified, taking into account the results of the acceptance and pilot testing, other design activities and circumstances related to the content of the submitted documentation. The project documentation must be actualized (updated) and the final versions submitted within the time limits agreed with the Contracting Authority, but no later than the date of submission of the final acceptance transfer certificate.
PR-22.	The final versions of the documents must be submitted in Confluence, MS Word or another format suitable for editing agreed with the Contracting Authority by uploading the document(s) to the agreed directory.
PR-23.	Preliminary (draft) versions must be submitted in electronic format by electronic means of communication. Comments and corrections in draft documents must be provided in Confluence with MS Office software package (or equivalent) track changes and commenting functionality. Versioning (version control) of the submitted documents must be carried out.
PR-24.	The Service provider will have to prepare the documentation indicated in Table 4 " Stages of the implementation of services".
PR-25.	All documents prepared by the Service provider will need to be approved by the Contracting Authority and the Maintenance Service provider. The detailed principles and timelines for the coordination of the documents will have to be set out and agreed in the Service provider's Terms of Service.
PR-26.	The final versions of the documents must be submitted in two formats: in an electronic format suitable for editing (.doc, .docx, .pdf or in another format agreed with the Contracting Authority) and with the signature (electronic or usual) signed by the responsible person of the Service provider (electronic or usual). Intermediate versions of documents are submitted only in electronic format.
PR-27.	All project documentation prepared by the Service provider must be approved by the responsible persons of the Contracting Authority. Detailed description is provided in the Rules of Procedure.
PR-28.	The Contracting Authority and other interested parties submit comments to the evaluated documentation: 1. no more than 10 working days for documents up to 100 pages. 2. during the period agreed with the Service provider, which is not less than 10 working days, for documents of more than 100 pages.

	3. After the Contracting Authority or other interested parties have submitted comments to the documentation being evaluated, the Service provider shall make corrections taking into account the following requirements: i. documents up to 100 pages must be corrected within a maximum of 5 working days. ii. documents larger than 100 pages must be corrected within a maximum of 10 working days. For the storage of source codes for the system, the Contracting Authority's code repository GitLab must be used.

6.4.2. Requirements for analysis and design

Requirement No.	Description
PR-29.	During the execution of the analysis and design stages, the Service provider must carry out a detailed analysis of business processes and needs and prepare detailed requirements analysis and design documents, which are detailed in section 6.4.1 "Requirements for documentation and its coordination" of the RPO.
PR-30.	The detailed requirements analysis document must include the use cases prepared in accordance with the functional and non-functional requirements of the Technical Specification and in accordance with the needs expressed by the Contracting Authority (use case diagrams and detailed descriptions of use cases, indicating steps (main, alternative, exceptional cases) and other restrictions using the Unified Modeling Language. Mapping of all functional and non-functional requirements of the Technical Specification to the content of the detailed analysis document (chapters, applications, diagrams, etc.) must be carried out. Mapping must be carried out in a form that makes it clear in what way each requirement of the RPO is designed and realized.
PR-31.	During the analysis and design, the Service provider shall conduct meetings with specialists appointed by the Contracting Authority and specialists of other relevant institutions.
PR-32.	During the detailed analysis and design stages, the Provider shall detail the functional and non-functional requirements of the RPO in order to implement the functionalities of the System that meet the needs.

6.4.3. Requirements for demonstrations

Requirement No.	Description
PR-33.	The Service provider must perform system demonstrations during the development phase after the end of each iteration by demonstrating the operation of the System live. A demonstration of the System, not a prototype, must be carried out.
PR-34.	The scope of the functionality displayed must be set out in the Terms of Reference for the Provision of Services. Before the start of the acceptance testing phase, the Contracting Authority must be demonstrated all the functionality of

	the System, except for that functionality that will be aligned as non-demonstratable (e.g. integration).
PR-35.	The purpose of the demonstrations is to familiarize the Contracting Authority with the software being developed and to receive feedback on the created (being developed) functionality.
PR-36.	Comments (feedback) may be made repeatedly during the validation testing phase, provided that they are not taken into account before the latter stage.
PR-37.	Feedback (comments) expressed during demonstrations must be recorded in the minutes of the meeting or in another agreed form (for example, in a specialized system for recording and tracking errors).
PR-38.	The demonstration of functionality must be carried out by the Service provider's specialists, during which the representatives of the Contracting Authority will be able to ask questions to the Service provider in order to objectively assess the possibilities of the functionalities demonstrated by the Service provider.
PR-39.	The demonstration must be carried out in Lithuanian or with translation into Lithuanian. Unless otherwise provided for in the project management plan.
PR-40.	If the Provider is unable to demonstrate the relevant functionalities due to technical obstacles, the demonstration could be postponed once for 1 business day, during which the Provider should remove technical barriers and perform a demonstration.
PR-41.	Functionality should be demonstrated in a working demonstration environment, i.e. not a video or similar.

6.4.4. Requirements for deployment

Requirement No.	Description
PR-42.	Before the start of the Deployment, the Service provider shall prepare a deployment plan (which shall be approved by the Contracting Authority), which shall include: 1. Responsibilities of the participants. 2. Description of deployment activities (deployment instruction). 3. Schedule of deployment activities. 4. Deployment scheme.
PR-43.	The deployment plan must describe and coordinate the steps for restoring the system in the event of an unsuccessful deployment of changes.
PR-44.	The deployment of the Software shall be carried out in the Contracting Authority's infrastructure at the time when the system is of the lowest use (e.g. outside working hours or on a weekend). The specific time(s) shall be agreed with the Contracting Authority.
PR-45.	The installation scheme must be established in accordance with the contracting authority's requirements for safety, speed, usability, etc.
PR-46.	After the installation, it must be ensured that all system components are working and are accessible from external networks, if necessary.
PR-47.	Regardless of the method of deployment of the solution, the Service Provider must prepare a common System deployment package (covering existing,

	modernized and new functions of the System), which the Contracting Authority could deploy independently at any time after the end of the Project.

6.4.5. Requirements for testing

Requirement No.	Description
PR-48.	Version tests of System (hereinafter referred to as "Testing") must be carried out.
PR-49.	The objectives of the testing are: 1. To make sure that all functional and non-functional requirements of the Technical Specification have been implemented. 2. To make sure that the implementation of the requirements has been carried out to the appropriate extent. 3. To determine whether the implementation of the requirements satisfies the Contracting Authority and other interested parties. 4. Identifying, registering and correcting functionality errors Bugs).
PR-50.	The Service provider shall prepare and agree with the Contracting Authority a testing plan containing: 1. testing methodology. 2. the responsibilities of the participants in the testing. 3. scope of testing. 4. testing environment. 5. the structure of the test scenarios. 6. schedule of testing activities. 7. data (conditions) required for testing. 8. the procedure for conducting testing and for recording and eliminating errors and deficiencies (functional inconsistencies). 9. test acceptance criteria. 10. other relevant information.
PR-51.	The following tests must be carried out: 1. Internal testing. Internal testing of individual components must be carried out by the Service provider without the participation of the representatives of the Contracting Authority, but evidence of such testing must be provided – internal testing reports, scripts for automatic tests (scripts must be uploaded to the Contracting Authority's code versioning system GitLab) and a list of identified inconsistencies. Internal testing must be performed in the Service provider's development environment. Automatic tests must be included in the automatic CI/CD processes. Internal testing activities must be carried out in accordance with the agreed Service Provision Regulation and testing scenarios developed by the Service provider in the Contracting Authority's testing management tool XRAY. 2. Load and performance testing. This testing must be carried out by the Service provider in its own development environment without the participation of representatives of the Contracting Authority. The results of this test must be reflected in the internal testing report. Additional load

	and performance testing will be carried out in the contracting authority's testing environment. If the test results performed by the Contracting Authority do not meet the specified requirements, the Service provider will have to carry out the necessary system optimization activities. 3. Integrity Testing. This testing must be carried out by the Service provider in a TEST environment with representatives of the Contracting Authority. The results of this test are necessary to make sure that the System Development Solution is ready for installation into the PROD environment. Errors and inconsistencies found during this testing must be eliminated and the corrected version of the System must be successfully tested in the TEST environment. 4. Acceptance Testing. This testing must be carried out in the TEST environment with the participation of the Service provider, the Contracting Authority and other interested parties: a. During this test, the implementation of the test objectives (determination of the level of implementation) must be checked. Acceptance testing activities must be carried out on the basis of the acceptance testing plan to be submitted by the Service provider, the acceptance testing scenarios developed by the Service provider in the Contracting Authority's testing management tool XRAY; The tests carried out shall ensure that the system version is suitable for pilot testing. b. During the testing, the recording of identified errors (problems) in electronic form log of the observed errors (problems) and their statuses must be carried out. Unless otherwise agreed, the errors must be recorded in the Contracting Authority's JIRA tool. c. When the provision of the Service includes testing (regardless of the environment) actions, the Service provider, in providing the service, must ensure (use) the resources necessary for testing (test data, including personal data, when testing cannot be performed with synthetic (unrealistic) personal data). d. The acceptance testing must be carried out on the basis of the hardware purchased by the Contracting Authority. e. The Service provider will be required to develop and provide all data, tools or other means necessary for testing. f. The Service provider will also have to compile other testing data that will be needed to verify the functional and non-functional requirements of the RPO. Other necessary test data, necessary measures and conditions must be detailed in the acceptance testing plan and agreed with the Contracting Authority. g. The acceptance test is completed when the criteria for acceptance of the test specified in the test plan are met.

	h. The tests carried out shall ensure that the system version is suitable for the pilot testing.
PR-52.	The Service provider will have to prepare processes for automated testing and deployment (Continuous Integration and continuous deployment) of the system itself and its constituent components in the GitLab tool used by the Contracting Authority.
PR-53.	CI/CD pipeline prepared by the Service provider and approved by the Contracting Authority must ensure: 1. Making artifacts. 2. Checking the quality of artifacts and code. 3. Verification of the security of artifacts and code (the Service provider will provide the tools necessary to check the security of the code). 4. Automatic execution of tests. 5. Deployment to the testing environment. 6. Deployment to the pilot testing environment. 7. Deployment to the production environment.
PR-54.	The Service provider may, on his own initiative, carry out any other tests and trials of the System (verification of source codes, verification of configuration, performance verification, high availability verification, expansion check, functionality verification, etc.) in order to ensure the quality of the system and compliance with the requirements. The Service provider will have to take into account the results of tests and tests carried out by the representatives of the Contracting Authority, provided in the JIRA system, to carry out the elimination of all deficiencies (violations, recommendations) indicated in the test results. The Service provider will have to create the necessary conditions for conducting scheduled tests and trials - provide a source code, provide login data to system components, create users necessary for testing, enable / disable system components, create access opportunities for specialized testing and testing software, perform other necessary activities that ensure the full-fledged execution of the testing and testing process.

6.4.6. Requirements for training

Requirement No.	Description
PR-55.	The supplier must prepare and agree with the Contracting Authority a training plan, training materials and provide the necessary environment for the training.
PR-56.	The training materials must include: 1. descriptions of the use of functionalities for individual user groups (based on user instructions). 2. animated instructions for use and / or visual (video) materials that allow to organize training for individual groups of users remotely.
PR-57.	Training materials must meet the following requirements: 1. all submitted materials must be divided according to the functional areas of the created software, prepared in Lithuanian and English and illustrated with the screenshots of the user interface.

	2. manuals must be complete and understandable to the reader while working individually, include all the intended functions of the system. 3. manuals must contain explanations of all fields of the created software. 4. administrators' manual must contain a detailed description of the import of data from other systems.
PR-58.	Training materials must be placed in places/directories agreed with the Contracting Authority and available after the Project.
PR-59.	Training must be carried out in a test or other environment specially prepared for training.
PR-60.	Number of contracting authority persons to be trained needs to be determined during preparation of training plan.
PR-61.	The place of training of the Users must be selected by the Service provider in prior agreement with the Contracting Authority (upon agreement, the training may also be carried out remotely). The costs associated with the training venue shall be the responsibility of the Service provider.

6.4.7. Requirements for pilot testing

Requirement No.	Description
PR-62.	The system must be subjected to a pilot testing aimed at ensuring the quality of the System, testing the production configuration of the system components, identifying and eliminating defects observed during the pilot testing, stabilizing the configuration of the working environment, taking into account the experience gained during the pilot testing.
PR-63.	Before the pilot testing, the Service provider prepare a pilot testing plan containing: 1. the scheme of communication between the participants of the pilot testing. 2. the responsibilities of the participants in the pilot testing. 3. a schedule of pilot testing activities. 4. the procedures for carrying out the pilot testing and for recording and correcting errors and deficiencies. 5. acceptance criteria for pilot testing.
PR-64.	The Service provider shall advise the Contracting Authority on the preparation of the pilot testing environment: 1. installation and configuration of system components. 2. migration (entry) of all necessary system data and removal of excess (not required for pilot testing) data.
PR-65.	The Contracting Authority shall ensure the operation of the system throughout the pilot testing, unless otherwise agreed.
PR-66.	During the test operation, the recording and elimination of identified errors (problems) must be carried out: 1. errors must be recorded in the Contracting Authority's error tracking tool - JIRA.

	2. The Service provider must immediately eliminate the system deficiencies within the time limits set out in the pilot testing plan, taking into account the errors recorded in the register of problems during pilot testing.
PR-67.	At the end of the pilot testing, the Service provider must prepare a report containing a summary of the errors found and corrected, providing information on other activities implemented during the pilot testing.
PR-68.	The Service provider will start system acceptance activities only after the System has met the acceptance criteria defined in the pilot testing plan.

6.5. Requirements for acceptance of the System

Requirement No.	Description
PR-69.	The final acceptance of the System or of the individual components of the System will take place after the pilot testing has been finished i.e. the acceptance can only take place once the acceptance criteria for the pilot testing have been met.
PR-70.	The Service provider must, before submitting the System to the Contracting Authority, provide the final versions of the documentation and the System source code, if they have been amended since the last delivery.
PR-71.	All Services will be accepted by signing the final acceptance-transfer act.
PR-72.	In order to ensure the smooth continuity of the Procurement: 1. The Service provider, without prejudice to the intellectual property rights of the copyright holder or third parties, contractually transfers to the Contracting Authority the property rights of the custom-made software and the prepared design documents, including, but not limited to, the right to use the created software for an unlimited period of time and without additional payment; the right to make copies of the created software; the right to modify and further develop the developed software; the right to transfer software to another technological platform; the right to use and modify the source code of the software created for it (the initial texts of the machine language); 2. if the software developed in the Project uses other software of the copyright holder or third parties, which is integrated into the custom-made software or is otherwise associated with the executed order and the author's property rights in the created software or the prepared design documents, its transfer to the Contracting Authority shall not restrict the right of the Service provider who has transferred these rights without the individual consent of the Contracting Authority for further development, improve, distribute and perform other necessary actions with the developed software or prepared design documents; 3. together with a computer program, as defined in the Law on Copyright and Related Rights of the Republic of Lithuania, the source code of the program is also transmitted to the Contracting Authority. The personal moral rights of the author of a computer program may not be used in a manner which restricts the rights of the holder of the copyright's property rights in this computer program, including the right to adapt, modify and distribute these works free of charge at his own discretion. The property

	rights of authors provided for in this paragraph, in accordance with the provisions of the Law on Copyright and Related Rights and Article 12 of the Law on the Management of State Information Resources, are transferred and granted in the territory of the Republic of Lithuania and EU countries for an indefinite period of time. 4. The Service provider shall transmit to the Contracting Authority developed System software, its source code or individual components of the System at the date of signing of the transfer deed. 5. The Service provider is not entitled to disclose any information relating to the provision of services to third parties without the written authorization of the Contracting Authority or if required to do so by law.

6.6. Requirements for warranty

Requirement No.	Description
PR-73.	The Service Provider after the date of signing the final Act of Transfer-Acceptance of Services will have to: 1. provide warranty for at least 12 months. 2. ensure the restoration of the system's operation in cases of complete or partial malfunction, including malfunctions caused by errors in the standard and non-standard software (except for cases caused by the fault of the Contracting Authority). 3. restore corrupted software components and data (except for cases caused by the fault of the Contracting Authority). 4. correct, free of charge, errors, inaccuracies and non-compliances for the requirements defined in the Technical Specification of the created or modified software and other solutions created or modified, as well as to prepare, test and prepare the updates necessary for installation in accordance with the procedures for the installation of updates developed by the Service provider and agreed with the Contracting Authority.
PR-74.	During the warranty, the Service provider must register system malfunctions and non-compliances in the problem / malfunction registration system (Service Desk) in accordance with the information and registration procedures agreed with the Contracting Authority.
PR-75.	During warranty, all errors, malfunctions and problems that have arisen and are identified must be classified: 1. Critical malfunction - the presence of an error and / or a problem that prevents the user from performing the required functions and no other alternative path to this function acceptable to the Contracting Authority is known. 2. Non-critical malfunction – when an error and / or problem has been identified that causes difficulties in using the System but does not affect the operation of the Functions of the System and has no other effect.
PR-76.	The main conditions for mandatory warranty: 1. reaction time to the problem (problem logged and forwarded for resolution) – no more than 15 minutes.

	2. Time it takes to resolve the problem: a. elimination of critical malfunctions – no more than 1 hour from the reception of the notification in the agreed manner. b. elimination of non-critical malfunctions – no more than 4 working hours from the reception of the notification in the agreed manner 3. if the error cannot be resolved within the prescribed period, another time for the resolution of the error shall be agreed with the Contracting Authority, with a justification for the time needed.
PR-77.	Consultations on identified inconsistencies and on software changes made by phone and e-mail (Hot line) – on weekdays from 8:00 to 17:00.
PR-78.	Possibility to register problems 24-hours online and monitor the state of problem solving using the error logging tool used by the Contracting Authority (unless during the project the parties agree to use the Service provider's error recording tool).
PR-79.	At the beginning of each quarter, the Service Provider will have to prepare a report on the execution of warranty supervision for the previous quarter within 5 working days.
PR-80.	The detailed procedure for warranty (methods of communication, procedures for installing updates, etc.) must be agreed with the Contracting Authority described in the warranty supervision regulation prepared by the Service Provider.

6.7. Requirements for Project management

Requirement No.	Description
PR-81.	The Service provider must ensure that all communication during the works takes place in Lithuanian. If experts from foreign countries are used, the Service provider must take care of the services of translation into Lithuanian at its own expense.
PR-82.	Procurement services must be implemented in a hybrid project implementation method. The duration of the stages (sprints) and the division of the works into sprints must be agreed by the Provider with the Contracting Authority.
PR-83.	The Service provider shall inform the Contracting Authority about the progress of the Performance of the Services and, at the request of the Contracting Authority, prepare presentations of the results of the service stages.
PR-84.	The Service provider must cooperate directly with the Contracting Authority, the Project partners and other interested parties of the Project.
PR-85.	The Service provider must submit and agree with the Contracting Authority the Regulation on the Provision of Services, which must detail the stages of the provision of services and their results (presentations), provide a detailed calendar schedule for the execution of works corresponding to the deadlines specified by the Contracting Authority, describe communication and risk management measures and the procedure for coordinating documents.
PR-86.	The Service provider shall prepare and submit to the Contracting Authority on a monthly basis interim reports on the provision of services containing: 1. information on the progress of the Service Contract.

	2. information about the risks and problems recorded during the reporting month. 3. information on the agreed changes in the change registry.
PR-87.	Interim reports on the provision of services must be submitted to the Contracting Authority within 5 working days from the end of the reporting period.
PR-88.	Upon completion of all works, the Service provider shall prepare a final report on the provision of services. The final report must be submitted to the Contracting Authority within 10 working days from the end of the last stage of the Provision of Services.

6.8. Requirements for change management

Requirement No.	Description
PR-89.	The requirements set out in the RPO, the Technical Specification or other annexes to the Service Agreement may be amended on the initiative of the Supplier or the Contracting Authority.
PR-90.	The appearance of changes may be caused by circumstances that arise or become known after the conclusion of the purchase agreement, their occurrence at the time of the submission of the tender or the conclusion of the purchase agreement could not be reasonably foreseen and controlled, as well as, it was not possible to reasonably foresee and control the risks of their occurrence in advance.
PR-91.	The change shall be formalized after the Service Provider and the Contracting Authority have approved the change in writing, in accordance with the terms of the Service Contract concluded between the Service Provider and the Contracting Authority and this Technical Specification, without prejudice to the principles of public procurement, in all of the following circumstances: 1. The effect of changing the functionality is documented, the degree of its criticality (non-essential, moderate, critical) and the consequences are described. 2. The change in functionality is not critical and does not affect the functionality of the technical solution as a whole. 3. change in functionality has been/ is marked on the testing plan and will be additionally tested. 4. changes in technical documentation, business processes and / or legal acts related to the change of functionality have been made. 5. The change in functionality is authorized (signed by a person authorized by the Contracting Authority). 6. The change in functionality is duly notified to all parties involved in the provision of the Services. 7. the changeable functionality does not complicate the achievement of the procurement goals. 8. all changes related to the functionality are entered in the registration log of the change of functionalities.

PR-92.	If the change in functionality is carried out without following the procedure set out in the previous paragraph, such a change in functionality is considered invalid.

6.9 Requirements for maintenance

Requirement No.	Description
PR-93.	Maintenance services will be provided upon receipt of the order of the Contracting Authority. The order will specify the period of the maintenance service.
PR-94.	Maintenance services shall be provided no earlier than the end of the warranty period and upon receipt of the order of the Contracting Authority.
PR-95.	Maintenance services must be provided on work days from 8:00 a.m. to 5:00 p.m., and if the malfunction of the System affects the ability of the Contracting Authority to provide services – at other times.
PR-96.	The Service provider must take into account that System (or components using its data) infrastructure (including standard software) can be updated, developed or modernized during the period of provision of the Services,
PR-97.	If the provision of maintenance services requires an update of the technical documentation of the System, it must be updated. The operating instructions for the system must also be updated and provided through the user interface of the software (giving the user the option to select the operating instructions from the software menu). The need to update the documentation must be assessed on a monthly basis.
PR-98.	If necessary, during the restoration of the System, maintenance services shall also be provided at another pre-agreed time in such a way that the terms of restoration of the System set by the Contracting Authority are not violated.
PR-99.	The Service provider shall designate the persons responsible for the provision of the maintenance services who must be available by the telephone number and e-mail provided during registration of tasks in the JIRA used by the Contracting Authority.
PR-100.	The Service Provider will have to organise all activities related to provision of services in such a way that all services ordered by the Contracting Authority, the results of the services provided by the Provider, their descriptions and other relevant information are registered in the Contracting Authority's JIRA. After the entry into force of the Contract, the Contracting Authority will provide the Service Provider's specialists with access to the created JIRA project.
PR-101.	The system is monitored by the Contracting Authority‘s tools. After the entry into force of the Contract, the Provider shall coordinate with the Contracting Authority the monitoring points of the System and the information about the observed issues, and the registration procedure.
PR-102.	The Provider must immediately record in the Contracting Authority's JIRA and/or notify the responsible persons appointed by the Contracting Authority of the observed or likely to occur malfunctions of the System, incidents (including electronic information security incidents) and problems and the expected deadlines for their elimination.

PR-103.	The decision on the importance of the ticket registered in the Contracting Authority's JIRA / Helpdesk and the assessment of whether the ticket has been properly resolved and can be closed is made by the Contracting Authority.
PR-104.	In the Contracting Authority's JIRA/Helpdesk, the Provider's representatives will be obliged to immediately report on the progress of the solution to the problem, and once a solution has been found and the problem has been resolved, to comment on the solution (see Table 5).
PR-105.	The time frame within which the Service Provider will be obliged to resolve the ticket will depend on the services provided by the Service provider and the priority given to these tickets by the Contracting Authority's specialists in terms of the impact of the disruption on the activities of the Contracting Authority (see Table 6).
PR-106.	The Critical, Major application priorities set by the contracting authority are not used for issues in testing and development environments. If new circumstances have been identified in the course of the investigation of the error, and a temporary alternative way of eliminating the problem has been agreed, the category of the appeal may be changed (reduced or increased) by agreement between the parties, indicating the reason for the change of priority.
PR-107.	The Service provider must resolve the ticket (provide the service and provide the deployment package if necessary) within the time limits set by the Contracting Authority, not including the time within which the ticket is clarified or provided by the Contracting Authority's specialists.
PR-108.	In all other cases, issues must be eliminated within the time agreed by the parties, and consultations shall be provided no later than by the end of the working day of submission of the inquiry, if it is submitted by electronic means and by 12 noon of that working day, in all other cases not later than by the end of the next working day. If the consultation cannot be provided by phone or e-mail.
PR-109.	If it is not possible to eliminate the malfunction within the specified time period (or within the time agreed by the parties), the Service provider must inform the Contracting Authority about it, submit and coordinate with it a malfunction elimination plan and continue to carry out the malfunction elimination actions in accordance with the deadlines provided for in the plan.
PR-110.	All errors and inconsistencies of the System software with its technical documentation and the requirements of additional development orders, deficiencies in the documentation, as well as all malfunctions of the System and their consequences, which have arisen after the installation of software changes made by the Service provider, shall be eliminated by the Service provider at its own expense.
PR-111.	Within the established ticket resolution deadlines, the Service provider will have to provide the necessary System software / deployment packages with installation instructions.
PR-112.	The Provider must consult the Contracting Authority's specialists and provide technical assistance using the Contracting Authority's JIRA tools, telephone, e-mail and the specialists' workplace: 1. If it is not possibile to provide a consultation immediately, the Service provider must provide answers to the consultation inquiries no later than

	within 8 (eight) working hours of the Contracting Authority (I - IV 8:00 - 17:00, V - 8:00 15:45), calculated from the submission of the consultation request to the Contracting Authority's malfunction resolution system. By agreement of the parties, this time limit may be extended for a reasonable period. Consultations may be provided by telephone, e-mail, by arriving at the specified premises of the Contracting Authority or by other means of communication agreed by the parties; 2. The primary and secondary level of customer consultation shall be ensured by the Contracting Authority, maintenance issues which cannot be resolved by the Contracting Authority shall be registered in the Contracting Authority's JIRA, assigning to the person specified by the Service provider.
PR-113.	The management of system events and tickets must be described in detail in the Regulation for the provision of services prepared by the Service provider.

Table 5. Ticket creation in Jira

Area	Event, message, order	JIRA type	JIRA label
Application Software	An unforeseen disruption, deterioration, or event that may disrupt the provision of the e-service. A malfunction or event of the registers and information systems which leads to an interruption of the provision of an electronic service or a deterioration in the quality of the service and which must be rectified within a specified period of time. There is a disturbance or imminent danger that the working capacity of the Registers and information systems will be disturbed according to an event observed by an automated tool, the Service Provider or a specialist of the Service Recipient. One or more recurring incidents that have a significant impact on the operation of the information system/registry, that have the same characteristics and that the reason for the incident is not known or requires in-depth analysis. If the problem is not addressed, incidents may recur. Performance issues. Analysis of issues.	Incidentas (to carry out the analysis) Bug (to identify the cause and eliminate the issue)	MedVAIS_Priežiūra_ Sutrikimas
Software change	Works related to the functionality, configuration or modification of running software.	Story	MedVAIS_Priežiūra_ Pakeitimas

Area	Event, message, order	JIRA type	JIRA label
	Technical debts e.g. code optimization works, integrity, reliability, security assurance and updates of technological solutions, that do not change the functionality of the system.	Technical Story	
Consultations	Advice or information to the specialists of the Centre of Registers on the software, functionality, its operation, technological solutions, development, administration of the workstations where these systems are installed, backup, restoration and operation monitoring, as well as advice or information on the system/register data and their management.	Paslaugos prašymas	MedVAIS_Priežiūra_ Konsultavimas
Data and document management service	Preparation of queries necessary for the collection of data of registers and information systems and collection of data according to the needs of the Centre of Registers. Updating the documentation.	Task	MedVAIS_Priežiūra_ Paslauga
Service provider suggestions	Proposals from the Service provider on technical or functional matters: proposals and conclusions on the needs for the development of registers and information systems and the improvement of the technical and technological architecture. Proposals for the Improvement of Service Provision and Service quality summary report and other relevant information. Review of system users' proposals, feedback, analysis, formulation of solutions.	Task	MedVAIS_Priežiūra_ Pasiūlymas

Table 6. Ticket priorities and resolution times

Type	Priority	Reaction time	Resolution time	Service mode	Service time
Incidentas Bug	Kritinis	Up to 15 min.	Up to 4 h.	24x7	0:00 – 24:00
	Aukštas	Up to 15 min.	Up to 6 h.	24x7	0:00 – 24:00
	Vidutinis	Up to 15 min.	Up to 1 working day.	8x5	8:00 – 17:00
	Žemas	Up to 15 min.	Up to 3 working days	8x5	8:00 – 17:00

7. SPECIAL REQUIREMENTS FOR THE PROVISION OF SERVICES

7.1. Safety requirements

7.1.1. Requirements for data protection and information security management

Requirement No.	Description
PR-114.	Data safety must be ensured in accordance with the Data Security Regulations of the System, the protection of personal data must be ensured on the basis of the Law on Legal Protection of Personal Data of the Republic of Lithuania and 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).
PR-115.	When providing the Services, the Service provider shall comply with and ensure that the Services comply with the security requirements set out in the Law on The Management of Information Resources of the State of the Republic of Lithuania, the Law on Cybersecurity of the Republic of Lithuania, Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 "On the Implementation of the Law on Cybersecurity of the Republic of Lithuania".
PR-116.	After the completion of the Procurement works, the data stored in the System must be protected from unauthorized access, use, alteration, disclosure, destruction or loss.
PR-117.	When designing the System, the Service provider shall coordinate with the Contracting Authority which protections and for which functionality of the System to use. The system must be protected from these threats: 1. security vulnerabilities and vulnerabilities in unauthenticated access. 2. unauthorized user session interception. 3. unauthorized interception or insertion of data. 4. code injection, XSS (Cross-site scripting). 5. other security breaches, the list of which is published in the Open Network Program Security Procurement (SSP); The Open Web Application Security Project (OWASP) website www.owasp.org).
PR-118.	In the event of a malfunction of the systems, appropriate notifications must be provided to the system users.
PR-119.	In the equipment used to provide the services, the Service provider shall, when developing the software, be guided by generally accepted standards of secure coding and good practices (SSA). The Open Web Application Security Project, OWASP) Secure Coding Practices or equivalent). The software being developed must not have unauthorized access to data and other security breaches that are identified in the latest list of IS security methodologies developed by the OWASP Testing Guide (not limited to OWASP Top 10 vulnerabilities) (https://www.owasp.org), the list of The OWASP API Security, etc. in the IS security methodologies developed by OWASP, or equivalent documents.
PR-120.	Security checks (threat simulations, source code reviews, other security checks provided in secure coding standards and good practice) must be carried out at each stage of software development in accordance with the Methodology for the Development of Electronic Services, approved by the Order of the Minister of

	Transport of the Republic of Lithuania of 7 October 2015, which sets out the requirements for penetration testing, which must be carried out from the entity engaged in the development of electronic services (provider) independent service provider. Security checks must be based on the security verification methods specified in generally accepted methodologies (OWASP application security verification standard, OWASP Testing Guide, Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), SANS, NIST SP 800-30" or equivalent security verification methodologies).
PR-121.	The supplier shall immediately inform about electronic information security incidents observed in the Contracting Authority's information technology infrastructure during the performance of the contract, inoperative or malfunctioning security measures, non-compliance with information security requirements, signs of criminal activity, information system security vulnerabilities, other security-critical events observed in the Contracting Authority's information technology infrastructure and, in agreement with the Contracting Authority, take appropriate measures, and actions to identify the causes of electronic information security incidents, to avoid the associated risks. Also, within the framework of its competence, to carry out all instructions and orders of the Contracting Authority's Safety Representative relating to the implementation of the safety policy.

7.1.2. Requirements for the application of safety legislation

Requirement No.	Description
PR-122.	The main security (both software and data) legislation that must be followed in the development of the System are: 1. 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 (GDPR)), security management standard LST ISO/IEC 27001:2017 "Information technology. Security methods. Information security management systems. Requirements", LST ISO/IEC 27002:2017 "Information Technology. Security methods. Information Security Controls Practice Regulations" and ISO/IEC 27701:2019 "Security Methods – ISO/IEC 27001 and ISO/IEC 27002 Supplement to Privacy Management – Requirements and Guidelines". 2. Law on Legal Protection of Personal Data of the Republic of Lithuania. 3. Law on Cybersecurity of the Republic of Lithuania. 4. Description of organizational and technical cybersecurity requirements applicable to cybersecurity entities, approved by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 "On the Implementation of the Law on Cybersecurity of the Republic of Lithuania. 5. Requirements for electronic information security of information systems, approved by Order No V-941 of the Minister of National Defense of the

	Republic of Lithuania of 4 December 2020 "On the approval of the Methodology for Conformity Assessment of Information Technology Security". 6. Description of the general requirements for electronic information security, approved by Resolution No. 716 of the Government of the Republic of Lithuania of 24 July 2013 "On the approval of the Description of the General Requirements for Electronic Information Security, the Description of the Guidelines on the Content of Security Documents and the Assessment of the Importance of Electronic Information Constituting the State Information Resources and the Description of the Guidelines for the Classification of State Information Systems, Registers and Other Information Systems"; 7. Recommendations of data reporting formats and standards approved by order No T-36 of 25 March 2013 of the Director of the Information Society Development Committee under the Ministry of Transport and Communications "On the approval of recommendations for data reporting formats and standards".

7.1.3. Data security requirements for the provision of services

Requirement No.	Description
PR-123.	Security of development and maintenance of information resources (secure coding, etc.) must be ensured as required by the Lithuanian standards LST EN ISO/IEC 27001 and LST EN ISO/IEC 27002LST ES ISO/IEC 27002.
PR-124.	The security requirements set out in the data security regulations for registers and information systems maintained by the contracting authority, in the documents implementing the security policy, in the description of the procedure for the management of cybersecurity and electronic information security incidents and in other legal acts (and in cases where such requirements change or arise after the signing of the public contract of sale).
PR-125.	Data security must be ensured: 1. ensuring the integrity, availability and confidentiality of data. 2. when registering the actions performed by the System users with the data, including the search and revision of data (it must be mandatory for the identified group of System users to enter the reason and / or legal basis for the actions performed in the system). 3. by providing a means for the System Administrator to verify the actions of System users. 4. providing safeguards against accidental erasure of data (e.g. warnings about intended erasure of data) and the approval of a delete action for multiple users (the "four-eyes principle"). This principle must be applied in operational and administrative applications. 5. for work with components, the System users are divided into groups according to the nature of the data processing, with some of them being given special rights (roles) to perform certain processing activities.

	Descriptions of system user groups and roles must be developed at the analysis and design stage. 6. information stored may not be deleted by any other means or under any circumstances other than those provided for at the analysis and design stages. 7. The Service provider must provide file formats that are allowed to be uploaded to the System and coordinate them with the Contracting Authority (e.g. it must not be allowed to attach potentially unsafe files that can automatically launch self-executive files).

7.1.4. Requirements for audit records

Requirement No.	Description
PR-126.	Audit record of System components (actions performed by users) and the operation of the components must be carried out.
PR-127.	An audit record management component must be implemented that would: 1. receive and accumulate data on the operation and use of the System. 2. realize the possibility to perform analysis of audit records (search, filtering according to various parameters). The necessary analytical actions with the audit records must be identified and agreed with the Contracting Authority during the execution of the analysis and design phases. 3. protect logs from unauthorised or unintentional alteration and deletion. 4. remove and archive audit records in accordance with the established rules, which must be agreed at the analysis and design stage. 5. enable to export the selected audit records.
PR-128.	When storing an audit record in a database, the following must be collected: 1. who performed the action (user). 2. when the action was taken (date, time). 3. what data was reviewed. 4. what data was updated. 5. what data was inserted. 6. user IP address. 7. what data has been removed. 8. what search phrases were used. 9. other information identified during the analysis and design phases.
PR-129.	Audit record of the data sent or received with internal and external systems through web services must be kept, including the information about: 1. system, register or database from which the data is received. 2. system, register or database to which the data is sent. 3. date and time of received or sent data. 4. sent or received data (if required); 5. other information identified during the analysis and design phases.

7.1.5. Requirements for risk, threat and vulnerability management

Requirement No.	Description
PR-130.	There must be risk, threat and vulnerability management: 1. The Service provider must follow recognized methodologies for the safe development of software, such as ISO/IEC 27034-1 or equivalent. 2. The Service provider must ensure that all employees involved in the development of the software are familiar with the methodologies for the safe development of the software. 3. The Service provider must perform an inspection to identify the main Security risks and security vulnerabilities of the System specified in the CWE/SANS TOP 25 Lists of Most Dangerous Software Errors OWASP 10 Most Critical Web Application Security Risks and to eliminate the risks and vulnerabilities found. After verification and elimination of risks / vulnerabilities, the Provider must provide a declaration stating that after the completion of the development works, the System does not contain the risks / vulnerabilities indicated in the TOP 25 of CWE/SANS and OWASP TOP 10 lists. 4. The Service provider must provide a list of all third-party components used in the system. 5. The Service provider must take appropriate action (Reasonable Effort) ensuring that third-party components meet the contracting authority's security requirements.
PR-131.	During the acceptance testing phase or during the pilot phase (or at any other agreed time), the Service provider shall provide all the necessary conditions for the specialists of the Contracting Authority's representatives who will carry out the penetration testing. If necessary, the Service provider will have to perform the configuration or programming work that will be necessary to test the security of the System in various scenarios for its use. The Service provider will not have to provide any software or hardware to run this test.
PR-132.	The Service provider shall carry out the necessary system programming and/or configuration works, taking into account the results of the penetration tests carried out by the contracting authority's representatives, in order to eliminate all identified important security vulnerabilities before the System is put into operation.

7.1.6. Requirements related to national security

Requirement No.	Description
PR-133.	The services offered by the Service provider must not pose a threat to national security. The Service provider, by submitting and signing the offer, confirms that the services it offers do not pose a threat to national security. The Contracting Authority will, in accordance with the procedure laid down in the Law on the Protection of Objects of Importance for National Security, apply to the Coordinating Commission for the Protection of Objects Of Importance to National

	Security (hereinafter referred to as the Commission) for verification of the conformity of the intended transaction with the interests of national security and in the event that the Commission requests the submission of additional documents to the Service Provider, the partners of the group of installers, and the sub-contractors involved by them will be obliged to submit them.
PR-134.	The Service provider, the partners of the group of entities, the economic entities whose capacities are relied on and the sub-contractors they employ shall not have any interest that could pose a threat to national security. The Contracting Authority, in accordance with the procedure established by the Law on the Protection of Objects Important for The Protection of National Security of the Republic of Lithuania, will apply to the Commission for verification of the conformity of the intended transaction with the interests of national security and in the event that the Commission requests the submission of additional documents to the Service Provider, partners of the group of entities, and the sub-contractors engaged by them will be obliged to submit them.
PR-135.	Maintenance or support of hardware or software may not be carried out from the states or territories specified in the list provided for in Article 92(14) of this Law on Public Procurement of the Republic of Lithuania (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).
PR-136.	The manufacturer of hardware or software or the person controlling it may not be registered (if the manufacturer or the person controlling it is a natural person – permanently residing or having citizenship) in the states or territories indicated in the list provided for in Article 92(14) of the Law on Public Procurement of the Republic of Lithuania (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).

7.1.7. Other security requirements

Requirement No.	Description
PR-137.	During the implementation of the project, all security and privacy measures currently used by the ESPBI IS will have to be maintained.
PR-138.	The provider must use the latest stable versions, fixes and patches of the software for the development of the system. During the deployment of the System into the production environment, it must be ensured that the system uses the latest stable versions of the software, provided that this does not change the essential principles of the architecture and functionality of the System, which are provided at the Design stage. Versions of software components that are in the testing stage or are officially announced by the software manufacturer that the software will no longer be supported, improved and/or developed from a certain date (End-of-life products) shall not be used.
PR-139.	Any unauthorized or undocumented remote or local access/accounts or any secret (undocumented) functionality that may compromise the security of the system is prohibited.
PR-140.	Secure configuration: 1. The provider must provide detailed instructions for configuring system and platform (OS, DBMS, Middleware) security.

	2. The System Provider must provide a list of platform components, system services, ports necessary for the functioning of the system. All components that are not necessary for the functionality of the System must be deactivated before the start of operation of the system.
PR-141.	Data flows between the different levels must be documented, indicating the ports and protocols required for communication, and limited by firewalls
PR-142.	The system must be accessible using the unified security measures provided by the ESPBI IS Security Subsystem, the "Single Sign-In" system. Single Sign On – (SSO) principle.
PR-143.	All identification information must be stored in an encrypted form in such a way that it is impossible to recover primary data (for example, passwords) from the stored information.
PR-144.	The Service provider undertakes to provide a System that is free of any hidden, security-impairing features, including: malware, viruses, "time mines", unauthorized access or features (Trojans, backdoors, easter eggs).
PR-145.	Messages from the integration interfaces must be encrypted signed with a SHA256 digital signature.
PR-146.	HTTP Cookie method or POST queries with hidden fields should be used for session management.
PR-147.	The system must generate system logs of user logins, access tests, and data traffic to monitor and respond to potential security incidents.
PR-148.	Links must be encrypted using strong encryption algorithms (e.g. AES-256).

8. Annexes

8.1. Annex 1. Order form for additional services

Annex 1

ORDER FOR ADDITIONAL SERVICES

(MedVAIS modernization services. Part II)

Contract No.		Order submission date	
Order No.		Expected completion date	
Order title		Estimated time effort	

Contracting Authority part. Service order description.

Annexes to the description	☐Yes	Number of attached pages:

Service Provider part. Description of order implementation.

Authorized Representative of the Contracting Authority

(name, surname, signature)

Authorized Representative of the Service Provider

(name, surname, signature)

PASLAUGŲ VIEŠOJO PIRKIMO TECHNINĖ SPECIFIKACIJA

I pirkimo objekto dalis

1. SĄVOKOS IR SUTRUMPINIMAI	
1.1. DB	Duomenų bazė
1.2. IS	Informacinė sistema
1.3. PĮ	Programinė įranga
1.4. Pirkimas	Perkančiosios organizacijos atliekamas viešasis pirkimas, skirtas šioje techninėje specifikacijoje nurodyto pirkimo objekto įsigijimui
1.5. Projektas	Projektas „Nacionalinės medicininių vaizdų archyvavimo ir mainų sistemos ir jos teikiamų elektroninių paslaugų plėtra"
1.6. MedVAIS	Nacionalinė medicininių vaizdų archyvavimo ir mainų sistema
1.7. Perkančioji organizacija, Pirkėjas, Užsakovas	Valstybės įmonė Registrų centras, juridinio asmens kodas 124110246, adresas Studentų g. 39, 08106 Vilnius. Perkančioji organizacija yra PVM mokėtoja
1.8. Sutartis	Su Pirkimo laimėtoju sudaryta Paslaugų viešojo pirkimo-pardavimo sutartis
1.9. Tiekėjas, Diegėjas	Asmuo (fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai) ar asmenų grupė, su kuriuo Perkančioji organizacija sudaro sutartį
1.10. Techninė specifikacija	Pirkimo techninė specifikacija
1.11. VNA	Nuo duomenis teikiančių sistemų nepriklausomas medicininių vaizdų ir su jais susijusių duomenų archyvas (angl. Vendor Neutral Archive)
1.12. DICOM	Standartas (ISO 12052:2017), aprašantis skaitmeninių medicininių vaizdų ir su jais susijusios informacijos tvarkymą, saugojimą ir apsikeitimo procesus, angl. Digital Imaging and Communications in Medicine.
1.13. Kitos šioje Techninėje specifikacijoje vartojamos sąvokos apibrėžtos yra apibrėžtos Sutartyje, Pirkimo sąlygose, Lietuvos Respublikos viešųjų pirkimų įstatyme, Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatyme, Mažos vertės pirkimų tvarkos apraše, patvirtintame Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 28 d. įsakymu Nr. 1S-97 „Dėl mažos vertės pirkimų tvarkos aprašo patvirtinimo, Numatomos viešojo pirkimo ir pirkimo vertės skaičiavimo metodikoje, patvirtintoje Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 27 d. įsakymu Nr. 1S-94 „Dėl Numatomos viešojo pirkimo ir pirkimo vertės skaičiavimo metodikos patvirtinimo", Lietuvos Respublikos civiliniame kodekse ir kituose viešuosius pirkimus reglamentuojančiuose teisės aktuose.	
2. BENDROS NUOSTATOS	
2.1. Šioje Techninėje specifikacijoje vartojami terminai „turi būti", „turi turėti", „turi leisti", „turi turėti galimybę", „bus", „leis", „apims" yra lygiaverčiai ir reiškia, kad Tiekėjas šio pirkimo apimtyje turi sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą ar suteikti atitinkamas paslaugas.	
2.2. Jeigu apibūdinant Pirkimo objektą, techninėje specifikacijoje yra nurodyti konkretūs modeliai ar šaltiniai, standartai, sertifikatai, protokolai, konkretūs procesai ar prekės ženklai, patentai, tipai, konkreti kilmė ar gamyba tai apima ir jiems lygiaverčius produktus ar procesus (t. y. tiekėjas gali siūlyti ir atitinkamus lygiaverčius produktus ar procesus), nepriklausomai nuo to, ar šalia yra prierašas „arba	

lygiavertis“ (sąlyga netaikytina, jeigu šaltinis, standartas, sertifikatas, protokolas, konkretus procesas ar prekės ženklas, patentas, tipas, konkreti kilmė ar gamyba nurodyta apibrėžiant Perkančiosios organizacijos ar partnerių turimus produktus ar esamus procesus). Lygiavertiškumo įrodymas yra tiekėjo pareiga. Pateikti minimalūs reikalavimai – Tiekėjai gali siūlyti geresnių charakteristikų Pirkimo objektą.

2.3. Paslaugų teikimui keliami bendrieji reikalavimai:

2.3.1. Tiekėjas pats pasirūpina Paslaugoms teikti reikalingomis priemonėmis ir technine įranga;

2.3.2. Tiekėjas neturi naudoti trečiųjų šalių komponentų, kurie yra nauji, niekada nenaudoti projektuose, Alpha ar Beta testavimo etapuose, reikalauja papildomų licencijų veikimui (angl. run-time licence);

2.3.3. Tiekėjas įsipareigoja Perkančiosios organizacijos atstovams teikti konsultacijas, susijusias su Pirkimo objektu, raštu bei žodžiu visą Sutarties galiojimo laikotarpį;

2.3.4. Perkančioji organizacija įsipareigoja visą Sutarties galiojimo laikotarpį teikti Tiekėjui būtiną ir reikalingą informaciją tinkamam Sutarties vykdymui;

2.3.5. Prieš suteikiant prieigą prie Perkančiosios organizacijos tvarkomų asmens duomenų, Tiekėjas privalės Perkančiajai organizacijai pateikti už asmens duomenų apsaugą atsakingo asmens vardą, pavardę ir kontaktinius duomenis (telefono numerį, el. pašto adresą);

2.3.6. Tiekėjas turės pasirašyti susitarimą dėl asmens duomenų tvarkymo, kaip tai nustatyta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas) 28 straipsnio 3 dalyje, kuriame turės būti nustatytas asmens duomenų tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšis ir duomenų subjektų kategorijos bei Registrų centro prievolės ir teisės;

2.4. Paslaugų teikimas turi būti vykdomas vadovaujantis žemiau nurodytais teisės aktais bei jų pakeitimais, atsiradusiais Paslaugų teikimo metu ir kitais su kompiuterizuojama veiklos sritimi bei kuriamomis ar modifikuojamomis el. paslaugomis susijusiais dokumentais:

2.4.1. Bendrasis duomenų apsaugos reglamentas (ES) 2016/679;

2.4.2. Lietuvos Respublikos viešųjų pirkimų įstatymas;

2.4.3. Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas;

2.4.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

2.4.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

2.4.6. Lietuvos Respublikos kibernetinio saugumo įstatymas;

2.4.7. Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimas Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo“;

2.4.8. Lietuvos Respublikos Vyriausybės 2001 m. balandžio 26 d. nutarimas Nr. 478 „Dėl Valstybės lėšų, skirtų valstybės kapitalo investicijoms, planavimo, tikslinimo, naudojimo, apskaitos ir kontrolės taisyklių patvirtinimo“;

2.4.9. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

2.4.10. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymu Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“;

2.4.11. Neįgaliesiems pritaikytų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių kūrimo, testavimo ir įvertinimo metodinės rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. gegužės 23 d. įsakymu Nr. T-72 „Dėl Neįgaliesiems pritaikytų interneto tinklalapių kūrimo, testavimo ir įvertinimo metodinių rekomendacijų patvirtinimo“;

2.4.12. Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2021 m. liepos 9 d. įsakymu Nr. V-484 „Dėl Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo".	
2.5. Tiekėjas privalo vadovautis Sutarties vykdymo metu aktualiomis teisės aktų redakcijomis. Tiekėjui privalomi ir visi Sutarties vykdymo metu naujai priimti / pakeisti teisės aktai, jeigu jie susiję su Sutarties įgyvendinimu. Jei naujai priimti / pakeisti teisės aktai prieštarauja šioje Techninėje specifikacijoje aprašytiems reikalavimams, Tiekėjas turi įgyvendinti reikalavimus vadovaudamasis Sutarties vykdymo metu priimtų / pakeistų teisės aktų aktualiomis versijomis.	
2.6. Tiekėjas atsako už Lietuvos Respublikoje galiojančių darbuotojų saugos ir sveikatos teisės aktų ir kitų darbuotojų saugą ir sveikatą darbe reglamentuojančių dokumentų reikalavimų vykdymą.	
3. PIRKIMO OBJEKTAS	
3.1. Pirkimo objektas	DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas (toliau – **Paslaugos**). Detalūs reikalavimai Paslaugoms nurodyti Techninės specifikacijos priede „Reikalavimai pirkimo objektui (I prikimo objekto dalis)"
3.2. Pirkimo objekto skaidymas	Pirkimo objektas neskaidomas į dalis. Neskaidymo priežastys nurodytos 3.3 p.
3.3. Pirkimo objekto neskaidymo į dalis pagrindimas (jei taikoma)	Pirkimo objektas negali būti skaidomas į dalis dėl: 1) **techninių priežasčių** – Pirkimo objektas apima vieno tipo paslaugų teikimą, t. y. DICOM standartu paremtų servisų ir VNA diegimą bei konfigūravimą, kurie yra glaudžiai susiję su MedVAIS išvystytais funkcionalumais. Naujų funkcionalumų vystymui ir integravimui pasirenkami sprendimai turi būti tarpusavyje technologiškai suderinti, o Pirkimo objektą skaidant į dalis ir skirtingiems tiekėjams vystant tą pačią IS, vieno tiekėjo naudojami sprendimai gali būti nesuderinami (arba sunkiai suderinami) su kito tiekėjo naudojamais sprendimais; 2) **dėl per didelių laiko sąnaudų** – Pirkimo objektą skaidant į dalis ir skirtingiems tiekėjams vystant tą pačią IS, tiekėjai, prieš pradėdami teikti savo paslaugų dalį, turėtų sulaukti kitų tiekėjų paslaugų teikimo rezultatų bei susipažinti su jais, o tai ženkliai padidintų galutinio rezultato pasiekimo terminus bei keltų riziką sklandžiam bei nenutrūkstamam IS darbui. Dviejų ar daugiau tiekėjų koordinavimas lemtų ženkliais didesnes laiko sąnaudas sprendimų ir procesų suderinimui Perkančiajai organizacijai, taip pat galimai turėtų įtakos užduočių atlikimo trukmės padidėjimui, kas galėtų pavėlinti galutinio rezultato pristatymą. 3) **papildomų kaštų** – skirtingų tiekėjų darbų koordinavimas ir jų atsakomybės ribų nustatymas pareikalautų papildomų administracinių išlaidų. Atsižvelgiant į tai, jog su tiekėju bus atsiskaitoma pagal valandinį įkainį, bet kokios tiekėjui tenkančios papildomos funkcijos, tokios, kaip papildoma analizė, bendradarbiavimas ir/ar teikiamų Paslaugų planavimas bei koordinavimas su kitais tiekėjais padidintų užduočių atlikimo darbo laiką, už kurį Perkančioji organizacija turėtų sumokėti papildomai, pagal valandinį įkainį. Skirtingų tiekėjų supažindinimas su projekto specifika, ESPBI IS architektūra

	ir vartotojų poreikiais reikštų papildomas sąnaudas. Taip pat kiekvienas tiekėjas turėtų atlikti dalį analizės ar pasirengimo darbų iš naujo, o tai lemtų dvigubą mokėjimą už tuos pačius procesus.
3.4. Mato vienetas	Komplektas Valanda Mėnesis
3.5. Paslaugų kiekis (apimtis)	1 komplektas (sistemos diegimas ir konfigūravimas) Iki 300 valandų (papildomų paslaugų užsakymai) 60 mėn. sistemos priežiūros paslaugos
3.6. Nurodytas Paslaugų kiekis (apimtis) yra	Maksimalus Paslaugos bus perkamos pagal poreikį, neviršijant maksimalaus nurodyto kiekio
3.7. Minimalus Paslaugų kiekis (apimtis), kurį įsipareigoja nupirkti Perkančioji organizacija Sutarties vykdymo metu (jeigu taikoma)	1 komplektas
3.8. Paslaugų kiekio (apimties) keitimas	Netaikoma
3.9. Paslaugų teikimo vieta	Paslaugos teikiamos nuotoliniu būdu, arba, esant poreikiui, Perkančios organizacijos padalinyje, esančiame Studentų g. 39, Vilniuje. Paslaugų teikimo vieta gali būti keičiama Vilniaus miesto ribose.
3.10. Paslaugų teikimo terminas	3.10.1. Paslaugos turi būti suteiktos ne vėliau kaip per 7 mėnesius nuo Sutarties įsigaliojimo dienos (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę ne mažiau kaip 7 mėnesiai) arba iki 2026-04-30 (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę mažiau kaip 7 mėnesiai). 3.10.2. Papildomas vystymo Paslaugos turi būti teikiamos nuo Sutarties įsigaliojimo dienos 7 mėnesius (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę ne mažiau kaip 7 mėnesiai) arba iki 2026-04-30 (tuo atveju, kai Sutarties sudarymo dieną iki 2026-04-30 yra likę mažiau kaip 7 mėnesiai). Paslaugų Užsakymai gali būti teikiami ir turi būti įvykdyti per Užsakyme nurodytą terminą, tačiau ne vėliau, nei iki aukščiau nurodyto termino pabaigos / datos. 3.10.3. Priežiūros paslaugos turės būti teikiamos (jei jos bus užsakytos) užsakytą laikotarpį, bet ne ilgiau kaip 60 mėnesių. Priežiūros paslaugos pradedamos teikti ne anksčiau nei pasibaigs garantinės priežiūros laikotarpis ir gavus Perkančiosios organizacijos užsakymą.
3.11. Paslaugų teikimo termino pratęsimas ir sąlygos	3.11.1. Paslaugų suteikimo terminas, nurodytas 3.10.1 p., gali būti pratęstas jei: 3.11.1.1. atsiranda įrodymais pagrįstų kliūčių ar trukdymų, kurių atsiradimui Sutarties šalys neturi įtakos ir už kuriuos jos neatsako, ir kurie sukelti ir priskirtini tretiesiems asmenims, ar kitų aplinkybių, kurių Sutarties šalys negalėjo iš anksto numatyti. Aplinkybės, kuriomis grindžiama būtinybė pratęsti Paslaugų suteikimo terminą, jokiu būdu

	negali priklausyti nuo Sutarties šalių. Kiekvienu tokiu atveju, Sutarties šalis, inicijuojanti Paslaugų suteikimo termino pratęsimą, raštu nedelsdama, bet ne vėliau kaip per 5 darbo dienas, apie tai praneša kitai Sutarties šaliai, pateikdama minėtų aplinkybių egzistavimo įrodymus. Nurodytas aplinkybes vertina kita Sutarties šalis, šiai sutikus, Paslaugų suteikimo terminas gali būti pratęsiamas tik minėtų aplinkybių egzistavimo laikotarpiui, tačiau ne ilgiau, kaip: 3.11.1.1.1. iki 2026-04-30; arba 3.11.1.2 Projekto įgyvendinimo terminui, jei Projekto įgyvendinimo terminas bus pratęstas, tačiau ne ilgiau, kaip 6 mėnesių laikotarpiui; arba 3.11.1.3. ne ilgesniam, kaip 6 mėnesių laikotarpiui tuo atveju, jei bus skirtas finansavimas ne iš Projekto lėšų. 3.11.2. Papildomų vystymo paslaugų suteikimo terminas, nurodytas 3.10.2. p., gali būti pratęstas, jei nebus išnaudota Pradinė Sutarties vertė. Tokiu atveju, Pirkėjas raštu apie tai praneša Tiekėjui, nurodydamas kokiam terminui siūloma pratęsti Paslaugų teikimo terminą. Tiekėjui sutikus, Paslaugų teikimo terminas gali būti pratęsiamas tik kol bus išnaudota Pradinė Sutarties vertė, bet ne ilgiau nei 6 mėnesių laikotarpiui (pratęsimų kiekis neribojamas).
4. TIEKĖJO ĮSIPAREIGOJIMAI	
4.1. Terminas per kurį Tiekėjas turi raštu informuoti Užsakovą apie bet kurias aplinkybes, kurios trukdo ir (ar) gali sutrukdyti Tiekėjui įvykdyti sutartinius įsipareigojimus Sutartyje nustatytais terminais bei tvarka	5 darbo dienos
4.2. Kiti Tiekėjo įsipareigojimai	-
4.3. Kiti Tiekėjo įsipareigojimai nurodyti Techninės specifikacijos priede „Reikalavimai pirkimo objektui“, Sutarties projekte ir Pirkimo sąlygose	
5. PASLAUGŲ PERDAVIMO IR PRIĖMIMO TVARKA	
5.1. Akto pasirašymo terminas	5 darbo dienos
5.2. Akto pasirašymo periodiškumas	5.2.1. Aktas pasirašomas po kiekvieno Techninės specifikacijos II dalyje "Reikalavimai pirkimo objektui" nurodyto etapo. 5.2.2. Suteiktų Papildomų paslaugų faktiniai kiekiai perduodami Užsakovui, Šalims pasirašant per praėjusį mėnesį suteiktų Papildomų paslaugų aktą. Papildomų paslaugų Aktas pasirašomas vieną kartą per mėnesį.
6. PASLAUGŲ KOKYBĖ	
6.1. Paslaugų garantinis terminas	12 mėn.
6.2. Paslaugų trūkumų pastebėtų Paslaugų perdavimo – priėmimo metu ar (ir) po Akto pasirašymo pašalinimo terminas	10 darbo dienų nuo informavimo apie pastebėtus trūkumus

7. SAUGUMO REIKALAVIMAI

7.1. Siekiant išvengti saugumo spragų ir pažeidžiamumų programinėje įrangoje, Tiekėjas, kurdamas PĮ ir teikdamas PĮ priežiūros paslaugas, turi vadovautis visuotinai pripažintais saugaus kodavimo standartais ir gerąja praktika (The Open Web Application Security Project (OWASP) Secure Coding Practices ir kt.). Kuriama PĮ neturi turėti nesankcionuotos prieigos prie duomenų ir kitų saugumo pažeidimų, kurie įvardijami naujausiame OWASP Testing Guide (neapsiribojant „OWASP Top 10" pažeidžiamumais) (https://www.owasp.org) sąraše, The OWASP API Security sąraše ir kt. OWASP parengtose IS saugumo metodikose arba lygiaverčiuose dokumentuose. Saugumo patikrinimai (grėsmių modeliavimai, išeities kodo pažiūros ir kt. saugaus kodavimo standartuose ir gerojoje praktikoje numatyti saugumo patikrinimai) turi būti vykdomi kiekviename PĮ kūrimo (vystymo, priežiūros) etape. Atliekant saugumo patikrinimus turi būti remiamasi naujausiomis šių metodikų versijomis: OWASP Web Security Testing Guide, Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), SANS, NIST SP 800-30" ar lygiavertėmis saugumo patikrinimo metodikomis.

7.2. Tiekėjas, suderinęs su Perkančiąja organizacija, turi naudoti naujai kuriamai PĮ jos kūrimo dieną esamas naujausias programinių paketų, bibliotekų, programavimo kalbų, jų kompiliatorių bei interpretatorių versijas.

8. APLINKOSAUGINIAI REIKALAVIMAI

8.1. Atsižvelgiant į tai, kad perkamos Paslaugos yra nematerialaus pobūdžio intelektinės paslaugos, nesusijusios su materialaus objekto sukūrimu, kurių teikimo metu nebus sukurtas neigiamas poveikis aplinkai, taip pat nebus sukuriamas taršos šaltinis ar generuojamos atliekos, vadovaujantis Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508, Pirkimas laikomas žaliuoju.

9. HIERARCHIJA

9.1. Ši Techninė specifikacija yra vientisas ir nedalomas dokumentas.

9.2. Techninės specifikacijos aiškinimo ir taikymo tikslais nustatoma tokia Pirkimo dokumentų viršenybės tvarka:

9.2.1. Skelbimas apie Pirkimą;
9.2.2. Sutarties specialioji dalis;
9.2.3. Techninė specifikacija;
9.2.4. Techninė specifikacijos priedas Nr. 1 „Reikalavimai pirkimo objektui";
9.2.5. Kiti Techninės specifikacijos priedai (jei taikoma);
9.2.6. Sutarties bendroji dalis;
9.2.7. Pirkimo sąlygos;
9.2.8. Pirkimo sąlygų priedai;
9.2.9. Tiekėjo pasiūlymas.

9.3. Jei bet kuriame iš 9.2 punkte nurodytų dokumentų yra dviprasmybių, neatitikimų ar prieštaravimų aukštesnės galios dokumentuose nustatytoms sąlygoms, šios visuomet yra laikomos turinčiomis viršenybę prieš žemesnės galios dokumente nustatytas sąlygas nuo jų nustatymo momento.

9.4. Tuo atveju, jei Tiekėjo pateikti dokumentai, įskaitant licencijas, jų naudojimo taisyklės ar pan., prieštarauja 9.2.1-9.2.8 p. nurodytuose dokumentuose nustatytoms sąlygoms, vadovaujamasi 9.2.1-9.2.8 p. nurodytų dokumentų nuostatomis.

10. KARTU SU PASIŪLYMU TIEKĖJAS TURI PATEIKTI

10.1. Rekomendacijas minimaliems infrastruktūros reikalavimams naujai sistemai ir medicininių vaizdų saugyklai. Rekomendacijose turi būti pateikta:

- Rekomendacijos pateikiamos skirtingiems sistemos naudojimosi segmentams: medicininių vaizdų kiekis per metus – 1, 2 ir 5 milijonai tyrimų per metus; DICOM peržiūros įrankio vartotojų skaičius vienu metu – 50, 100 ir 300 vartotojų vienu metu;
- Planuojamas sistemos serverių kiekis, jų paskirtis (aplikacijų ir duomenų bazės serveriai) ir reikalingi

resursai (CPU, RAM, disko talpa); - Techniniai reikalavimai medicininių vaizdų saugyklų technologijoms; - Kur įmanoma turi būti išskirti minimalūs ir rekomenduotini resursų reikalavimai; - Kita informacija, kuri tiekėjo atžvilgiu gali būti naudinga planuojant infrastruktūrą naujai sistemai ir medicininių vaizdų saugyklai.	
11. PRIEDAI	
11.1. Priedas Nr. 1	Reikalavimai pirkimo objektui

IS modernizavimo paslaugų pirkimo
sąlygų
Techninės specifikacijos
1 priedas

REIKALAVIMAI PIRKIMO OBJEKTUI
I PIRKIMO OBJEKTO DALIS
DICOM STANDARTU PAREMTŲ SERVISŲ IR VNA DIEGIMAS BEI KONFIGŪRAVIMAS

Turinys

1. PIRKIMO TIKSLAS IR UŽDAVINIAI 3
1.1. Santrauka 3
1.2. Sąvokos ir sutrumpinimai 3
1.3. IS modernizavimą bei veikimą ir Paslaugų teikimą reglamentuojantys teisės aktai 5
1.4. Pirkimo uždaviniai 6
1.5. Sprendžiamų problemų aprašymas 7
2. ESAMOS BŪSENOS APRAŠYMAS 8
2.1. Sistemos organizacinė struktūra 9
2.2. Sistemos naudotojai ir tikslinės grupės 9
2.3. Sistemos funkcinė struktūra architektūrai 10
2.3.1. Sistemos loginis modelis 11
2.3.2. Naudojamos technologijos 15
2.4. Sistemos fizinė struktūra 15
3. SISTEMOS PAGEIDAUJAMOS BŪSENOS APRAŠYMAS 16
4. FUNKCINIŲ REIKALAVIMŲ APRAŠYMAS 17
4.1. Bendrieji reikalavimai 18
4.2. Funkciniai reikalavimai Sistemai 20
5. NEFUNKCINIŲ REIKALAVIMŲ APRAŠYMAS 23
5.1. Kriterijai nefunkcinių reikalavimų įgyvendinimui 23
5.2. Reikalavimai Sistemos architektūrai 24
5.3. Reikalavimai medicininių vaizdų peržiūros įrankiui 25
5.4. Reikalavimai, susiję su duomenų registro ir duomenų saugyklos valdymo įrankiu 26
5.5. Reikalavimai technologijoms 26
5.6. Reikalavimai Sistemos prieinamumui 27
5.7. Reikalavimai plečiamumui 27
5.8. Reikalavimai rezervinių kopijų darymui ir atstatymui 28

5.9. Reikalavimai sistemos monitoringui ... 28
5.10. Reikalavimai duomenų modeliui ... 29
5.11. Reikalavimai Sistemos administravimui ... 30
5.12. Reikalavimai našumui ir greitaveikai ... 30
5.13. Reikalavimai programinei įrangai ir programinės įrangos licencijoms ... 32
5.14. Reikalavimai integracinėmis sąsajoms ... 34
5.15. Reikalavimai naudotojų sąsajai ir patogumui naudoti ... 34
5.16. Reikalavimai duomenų archyvavimui ... 35
5.17. Reikalavimai standartų taikymui ... 36
6. REIKALAVIMAI PASLAUGŲ TEIKIMUI ... 36
6.1. Reikalavimai darbo vietai ... 36
6.2. Reikalavimai paslaugų užsakymui ... 37
6.3. Reikalavimai RPO įgyvendinimui ... 38
6.4. Reikalavimai paslaugų teikimo etapams ir programinės įrangos kūrimo iteracijoms ... 40
6.4.1. Reikalavimai dokumentacijai ir jos derinimui ... 52
6.4.2. Reikalavimai analizei ir projektavimui ... 53
6.4.3. Reikalavimai demonstracijoms ... 53
6.4.4. Reikalavimai diegimui ... 54
6.4.5. Reikalavimai testavimui ... 54
6.4.6. Reikalavimai mokymams ... 57
6.4.7. Reikalavimai bandomajai eksploatacijai ... 58
6.5. Reikalavimai Sistemos priėmimui ... 58
6.6. Reikalavimai garantinei priežiūrai ... 60
6.7. Reikalavimai Projekto valdymui ... 61
6.8. Reikalavimai pakeitimų valdymui ... 61
6.9. Reikalavimai priežiūros paslaugų teikimui ... 62
7. SPECIALIEJI REIKALAVIMAI PASLAUGŲ TEIKIMUI ... 66
7.1. Reikalavimai saugai ... 66
7.1.1. Reikalavimai duomenų apsaugai ir informacijos saugumo valdymui ... 66
7.1.2. Reikalavimai saugą reglamentuojančių teisės aktų taikymui ... 68
7.1.3. Paslaugų teikimo duomenų saugos reikalavimai ... 69
7.1.4. Reikalavimai auditavimui ... 69
7.1.5. Reikalavimai rizikų, grėsmių ir pažeidžiamumų valdymui ... 70
7.1.6. Reikalavimai susiję su nacionaliniu saugumu ... 71
7.1.7. Kiti saugos reikalavimai ... 72
8. PRIEDAI ... 73
8.1.1 priedas. Papildomų paslaugų užsakymo forma ... 73

1. PIRKIMO TIKSLAS IR UŽDAVINIAI

1.1. Santrauka

1. Nacionalinės medicininių vaizdų archyvavimo ir mainų informacinės sistemos (toliau MedVAIS arba Sistema) modernizavimo paslaugų pirkimo sąlygų techninės specifikacijos reikalavimų pirkimo objektui (toliau – Reikalavimai pirkimo objektas arba RPO) pateikiami reikalavimai, pagal kuriuos turi būti modernizuojama Sistema.

2. RPO pateikiama informacija apie teisės aktus ir standartus, kuriais turi vadovautis Sistemos modernizavimo paslaugų Teikėjas modernizuojant Sistemą, įvardijami Pirkimo uždaviniai, pateikiama numatoma Sistemos funkcinė architektūra ir jos aprašymas, aprašoma siekiama būsena bei nurodomi funkciniai ir nefunkciniai reikalavimai, modernizuojant Sistemą.

3. Šio pirkimo objekto dalyje numatyta:

3.1 Atnaujinti DICOM standarto palaikymą ir integraciją užtikrinant DICOM ir ne DICOM vaizdų ir jų metaduomenų valdymą per standartizuotus DICOMweb (pvz.: QIDO-RS, WADO-RS, STOW-RS) ir DIMSE (pvz.: C-FIND, C-MOVE, C-STORE) protokolus.

3.2 DICOM vaizdų peržiūros įrankio integracija, leidžianti vartotojams peržiūrėti medicininius vaizdus.

3.3 Gamintojui neutralaus archyvo (angl. Vendor neutral archive, VNA) integracija – užtikrinamas standartizuotas medicininių vaizdų ir susijusių duomenų perdavimas ir laikymas, nepriklausomai nuo gamintojo ar specifinės diagnostikos įrangos.

1.2. Sąvokos ir sutrumpinimai

4. RPO naudojamos sąvokos ir sutrumpinimai pateikti 1 lentelėje „Naudojamos sąvokos ir sutrumpinimai".

1 lentelė. Naudojamos sąvokos ir sutrumpinimai

Sąvoka/sutrumpinimas	Paaiškinimas
DEV	RC informacinių technologijų infrastruktūros kūrimo (angl. Development environment) aplinka, kurioje vyksta sistemos kūrimas ir vidinis testavimas
Testavimo aplinka	RC informacinių technologijų infrastruktūros aplinka, skirta programinei įrangai testuoti (angl. Testing environment), kurioje vyksta sistemos priėmimo testavimas
Vystymo aplinka	RC infrastruktūros aplinka skirta kūrimo bei vystymo darbams vykdyti (angl. Development environment)
WS, web service	Žiniatinklio paslauga (angl. web service)
PA	Panaudos atvejis
ASPĮ	Asmens sveikatos priežiūros įstaiga
ESPBI IS	Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistema
HIS	Sveikatos priežiūros įstaigos informacinė sistema

Sąvoka/sutrumpinimas	Paaiškinimas
Projektas	Nacionalinės medicininių vaizdų archyvavimo ir mainų sistemos (MedVAIS) ir jos teikiamų elektroninių paslaugų plėtra
RC, Perkančioji organizacija	Valstybės įmonė Registrų centras
SAM	Lietuvos Respublikos sveikatos apsaugos ministerija
SPĮ	Sveikatos priežiūros įstaiga
SPS	Sveikatos priežiūros specialistas
SVEIDRA IS	Privalomojo sveikatos draudimo informacinė sistema
VLK	Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos
IS	Informacinė sistema
IT	Informacinės technologijos
Portalas arba E. sveikatos portalas	Priemonių visuma, skirta pacientų ir sveikatinimo specialistų prieigai prie Elektroninių paslaugų. ESPBI IS aplinkoje Portalą įgyvendina E. sveikatos portalo posistemė (toliau – E. sveikatos portalo posistemė). Pastaba: Portalas įgyvendina E. sveikatos portalo koncepciją, apibrėžtą E. sveikatos plėtros programoje ir architektūros modelyje.
XML	Bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba arba šios kalbos failas (angl. Extensible Markup Language)
DICOM	Standartas (ISO 12052:2017), aprašantis skaitmeninių medicininių vaizdų ir su jais susijusios informacijos tvarkymą, saugojimą ir apsikeitimo procesus, angl. *Digital Imaging and Communications in Medicine*.
FHIR	Tarptautinė el. sveikatos srities standartizuota metodologija (ISO/CD PAS 24305), angl. *Fast Healthcare Interoperability Resources*.
MedVAIS arba Sistema	Nacionalinė medicininių vaizdų archyvavimo ir mainų informacinė sistema.
PACS	Medicininių vaizdų archyvavimo ir mainų informacinė sistema, angl. *Picture Archiving and Communication System*.
RIS	Sveikatos priežiūros įstaigos radiologinio padalinio informacinė sistema, angl. *Radiology Information System.*
UID	Unikalus objekto identifikatorius DICOM standarte, angl. *DICOM Unique Identifier*.
Papildomos paslaugos	Papildomai reikalingos suteikti paslaugos, suderinamos tarp Paslaugų teikėjo ir Perkančiosios organizacijos Projekto vykdymo metu
Paslaugų teikėjas	Projekto vykdymo paslaugų teikėjas, kuris paslaugas teikia vadovaudamasis šia Technine specifikacija
MV	Medicininis(-ai) vaizdas(-i)

5. Kitos RPO vartojamos sąvokos apibrėžtos žemiau išvardintuose teisės aktuose.

1.3. IS modernizavimą bei veikimą ir Paslaugų teikimą reglamentuojantys teisės aktai

6. Lietuvos Respublikos sveikatos sistemos įstatymas;
7. Lietuvos Respublikos sveikatos draudimo įstatymas;
8. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
9. Lietuvos Respublikos kibernetinio saugumo įstatymas;
10. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudojimo tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. gegužės 26 d. įsakymu Nr. V-657 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudojimo tvarkos aprašo patvirtinimo";
11. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimu Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo";
12. Sveikatos priežiūros įstaigų informacinių sistemų susiejimo su e. sveikatos paslaugų ir bendradarbiavimo infrastruktūra reikalavimai ir techninės sąlygos, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2010 m. gruodžio 17 d. įsakymu Nr. V-1079 „Dėl sveikatos priežiūros įstaigų informacinių sistemų susiejimo su e. sveikatos paslaugų ir bendradarbiavimo infrastruktūra reikalavimų ir techninių sąlygų patvirtinimo";
13. Skaitmeninės sveikatos sistemos funkcinės, techninės ir programinės įrangos architektūros aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2019 m. spalio 2 d. įsakymu Nr. V-1119 „Dėl Skaitmeninės sveikatos sistemos funkcinės, techninės ir programinės įrangos architektūros aprašo patvirtinimo";
14. Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. liepos 4 d. įsakymas Nr. V-769 „Dėl duomenų subjektų teisių įgyvendinimo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinėje sistemoje tvarkos aprašo patvirtinimo";
15. Lietuvos Respublikos sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymas Nr. 515 „Dėl sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarkos";
16. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;
17. ESPBI IS nuostatai koreguojami vadovaujantis Informacinių sistemų steigimo, kūrimo, atnaujinimo, pertvarkymo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimu Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo";
18. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymu Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo";
19. Elektroninių paslaugų kūrimo metodika, patvirtinta Lietuvos Respublikos susisiekimo ministro 2015 m. spalio 7 d. įsakymu Nr. 3-416(1.5E) „Dėl metodinių dokumentų patvirtinimo";
20. Duomenų teikimo formatų ir standartų rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. kovo 25 d. įsakymu Nr. T-36 „Dėl Duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo";
21. ESPBI IS techninis aprašymas (specifikacija) rengiamas patvirtinus atnaujintus ESPBI IS nuostatus. ESPBI IS techninis aprašymas (specifikacija) rengiamas vadovaujantis Informacinių sistemų steigimo, kūrimo, atnaujinimo, pertvarkymo ir likvidavimo tvarkos aprašu, patvirtintu

Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimu Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo";
22. Kuriamų viešųjų ir administracinių elektroninių paslaugų tinkamumo naudotojams užtikrinimo priemonių metodinėmis rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. gegužės 5 d. įsakymu Nr. T-65 „Dėl Kuriamų viešųjų ir administracinių elektroninių paslaugų tinkamumo naudotojams užtikrinimo priemonių metodinių rekomendacijų patvirtinimo";
23. Projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2017 m. lapkričio 22 d. įsakymu Nr. T-126 „Dėl projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijų patvirtinimo";
24. Neįgaliesiems pritaikytų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių kūrimo, testavimo ir įvertinimo metodinės rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2004 m. kovo 31 d. įsakymu Nr. T-40 „Dėl Neįgaliesiems pritaikytų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių kūrimo, testavimo ir įvertinimo metodinių rekomendacijų patvirtinimo";
25. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);
26. Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo";
27. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo";
28. Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2017 m. lapkričio 22 d. įsakymas Nr. T-126 „Dėl projektų, kurių įgyvendinimo metu kuriamos elektroninės paslaugos ir informacinių technologijų sprendimai, techninės priežiūros rekomendacijų patvirtinimo".
29. Kiti teisės aktai, reglamentuojantys valstybės informacinių sistemų veikimą, duomenų saugą, funkcijas;
30. Jeigu Sutarties vykdymo metu būtų pakeisti išvardyti ar kiti, su šioje Techninėje specifikacijoje numatytų reikalavimų įgyvendinimu, susiję, teisės aktai, Teikėjas privalo atsižvelgti į šiuos pakeitimus, jeigu apie juos buvo sužinota iki projektavimo etapo pabaigos. Jeigu teisės aktų pakeitimai buvo priimti, tai laikoma, kad Teikėjas privalėjo sužinoti apie tokius pakeitimus. Jeigu teisės aktų pakeitimai dar nepriimti, o yra tik rengimo, svarstymo ar priėmimo etape, tai laikoma, kad Teikėjas sužinojo apie tokius pakeitimus tik tada, kai Perkančioji organizacija jį informavo ir pareikalavo tokius pakeitimus įdiegti;
31. Teikėjas privalo vadovautis ne tik aukščiau išvardintais, bet ir visais kitais su Sutarties įgyvendinimu susijusiais teisės aktais, taip pat jų naujausiais pakeitimais ir papildymais. Teikėjas turi vadovautis Sutarties vykdymo metu naujai priimtais teisės aktais, jeigu jie susiję su Sutarties įgyvendinimu ir yra priimti ne vėliau kaip iki projektavimo etapo pabaigos.

1.4. Pirkimo uždaviniai

32. Pirkimo uždaviniai:

32.1. Atlikti detalią poreikių ir galimybių analizę;

32.2. Sumodeliuoti ir suprojektuoti modernizuojamos ESPBI IS MedVAIS posistemės funkcionalumą ir duomenų mainų sąsajas;

32.3. Parengti ir suderinti visą numatytą Sistemos dokumentaciją;

32.4. Realizuoti Sistemos funkcijas ir duomenų mainų sąsajas;

32.5. Įdiegti Sistemos funkcijas ir duomenų mainų sąsajas;

32.6. Įdiegti duomenų bazes bei kitą reikiamą standartinę programinę įrangą;

32.7. Sėkmingai įvykdyti Sistemos sukurtų funkcijų ir sąsajų priėmimo testavimą;

32.8. Parengti mokymų medžiagą ir įvykdyti mokymus;

32.9. Paruošti Sistemą eksploatavimui;

32.10. Sėkmingai atlikti sukurtos Sistemos bandomąją eksploataciją.

33. Perkamų paslaugų rezultatai:

33.1. Sukurta, įdiegta ir ištestuota modernizuota ESPBI IS su atnaujinta MedVAIS posisteme;

33.2. Sukurtos sąsajos su išorinėmis informacinėmis sistemomis ir registrais;

33.3. Parengta Sistemos techninė dokumentacija;

33.4. Apmokyti Sistemos naudotojai;

33.5. Suteikta Sistemos garantinė priežiūra.

1.5. Sprendžiamų problemų aprašymas

34. MedVAIS architektūra yra apribota konkrečios ASPĮ deklaruotų ir pateiktų MV turiniu, todėl nėra galimybės sudaryti kelių ASPĮ sukurtų MV sąrašų pagal diagnozes, kūno vietas ar konkretų pacientą. Duomenų apie tuos MV, kurie nėra deklaruojami ir/arba perduodami saugoti į MedVAIS, nacionaliniu mastu nėra, taigi, nėra prieigos prie šių MV duomenų sveikatos priežiūros paslaugų teikimo ir pakartotinio naudojimo tikslais.

35. Esami MV paieškos parametrai riboja analitikos galimybes, kylančias iš skirtingų sveikatos priežiūros specialistų poreikių.

36. Nėra sukurtas pilnas MV nuasmeninimo ir pseudoniminimo funkcionalumas, kuris pralėstų MV duomenų pakartotinio panaudojimo galimybes.

37. MedVAIS nėra galimybės atlikti saugykloje esančių MV WEB peržiūros, o ASPĮ gydytojai per e. sveikatos portalą negali atsisiųsti savo ASPĮ sugeneruotų diagnostinių tyrimų į savo darbo stotis.

38. Esamas medicininio vaizdo aprašymo struktūros duomenų laukai nesusieti su klasifikatoriais ir jose unifikuotomis kintamųjų reikšmėmis, kas nepagrįstai prailgina aprašymo kūrimo procesus.

39. Esamame aprašyme nėra visų Europos komisijos rekomendacijose nurodytų duomenų laikų, naudojamų dokumento paieškai.

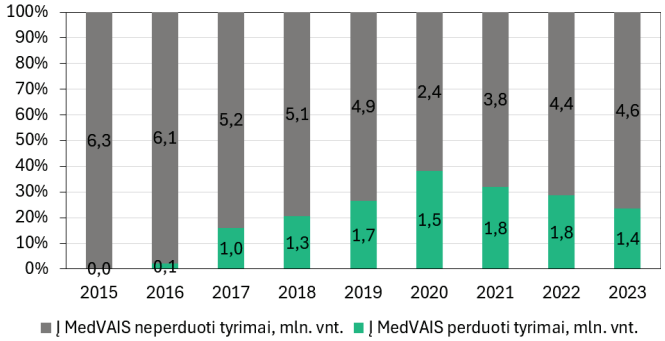
40. Šiuo metu MedVAIS posistemė naudoja ESPBI IS naudotojų prieigos teisių prie pacientų ESI įrašų modulį. Šis modulis nėra tinkamas praktikoje įprastose MV situacijose: MV sukuria vienos ASPĮ specialistai, o šio MV aprašymą parengia kitos ASPĮ gydytojai. Šiuo metu MedVAIS MV gali būti patvirtintas tik deklaruojant/perduodant MV ir jo aprašymą kartu, t.y. autorizuojantis iš vienos ASPĮ. Todėl MedVAIS būtina modernizuoti, sukuriant praktikoje įprastai situacijai pritaikytą naudotojų teisių valdymo algoritmą.

41. Šiuo metu MedVAIS saugomi ne visi sveikatos priežiūros paslaugų teikimo metu sukuriamų MV tipai: pavyzdžiui, nėra saugomi jpg, kurie yra gydytojams-dermatologams svarbūs MV, taip pat

kraujospūdžio matavimai, atliekami HOLTER aparatais, duomenys, miego stebėjimo duomenys ir pan.

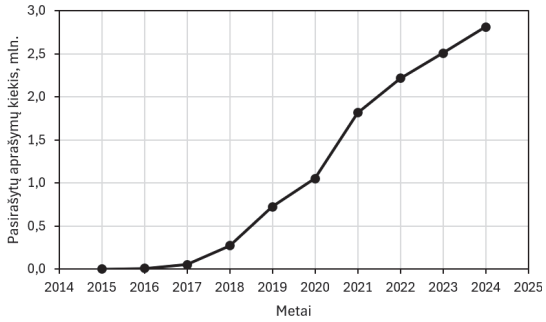
2. ESAMOS BŪSENOS APRAŠYMAS

42. Nacionalinė MV archyvavimo ir mainų IS MedVAIS buvo sukurta 2013-2015 m. kaip atskira ESPBI IS posistemė, skirta saugoti, archyvuoti ir dalintis medicininiais vaizdais tarp ASPĮ:
42.1. MedVAIS sukurtoje infrastruktūroje sukaupti 24 tipų radiologiniai, ultragarso ir ECG tyrimų rezultatų skaitmeniniai MV.
42.2. Remiantis Higienos instituto duomenimis, rentgeno (XA), ultragarso (US), kompiuterinės tomografijos (CT), magnetinio rezonanso (MR), endoskopijos (ES) ir pozitronų emisijos kompiuterinės tomografijos (PT) tyrimai Lietuvoje kasmet sudaro apie 6 mln. Laikant, kad: XA – 90 MB, US – 60 MB, CT – 430 MB, MR – 115 MB, ES – 30 MB, PT – 30 MB bendras sugeneruojamų tyrimų kiekis Lietuvoje yra ~ 600 Tb per metus, iš kurių į MedVAIS perduodama 20 – 25 %.
42.3. Į MedVAIS per metus perduodama iki 1,8 mln. tyrimų. Tai sudaro nuo kelių iki ~ 40 % medicininių vaizdų 2015 – 2023 metų laikotarpyje.



1 pav Medicininių vaizdų kiekis MedVAIS ir Lietuvoje 2015 – 2023 metais.

42.4. Iki 2023 m. pabaigos – MedVAIS buvo saugoma daugiau nei 15 mln. MV. Bendra MedVAIS saugomų MV užimama talpa 2024 m. pabaigoje buvo 1,4 PB, kai visa MV saugojimui skirtos infrastruktūros talpa 2,3 PB.
42.5. Kiekvienas medicininis vaizdas MedVAIS yra susietas su atskiru ESI įrašu, t.y. duomenų rinkiniu E027-va „Medicininio vaizdo diagnostinis aprašymas", kurio struktūra pateikiama 3-ioje lentelėje.
42.6. Per MedVAIS gyvavimą iki 2024 metų pabaigos buvo pateikta virš 11 mln. pasirašytų medicininio vaizdo aprašymo formų.



2 pav. Pasirašytų ir į MedVAIS perduotų medicininio vaizdo aprašymo formų kiekio kitimas 2015 – 2024 metais.

42.7. Šiuo metu ~ 200 įstaigų yra integravusios į MedVAIS (įstaigos PACS siunčia medicininius vaizdus į MedVAIS).

42.8. MedVAIS posistemė buvo sukurta užtikrinti šias galimybes:
42.9. ASPĮ ir specialistams elektroniniu būdu gauti kitų ASPĮ diagnostinių tyrimų rezultatus.
42.10. Medicininį vaizdą sukūrusiai ASPĮ per e. sveikatos portalą teikti diagnostinį tyrimą elektroniniu būdu kitos ASPĮ specialisto analizei.
42.11. Peržiūrėti MedVAIS esančius medicininius vaizdus pacientams, sveikatos priežiūros specialistams, sveikatos priežiūros paslaugų valdymą ir kontrolę vykdančios organizacijoms.
42.12. Gauti ir peržiūrėti statistines ataskaitas bei statistinius duomenis.
42.13. Gauti nuasmenintą medicininį vaizdą sveikatos priežiūros paslaugų valdymui ir kontrolei bei mokslinei veiklai.

2.1. Sistemos organizacinė struktūra

43. Sistemos valdytojas yra Lietuvos Respublikos sveikatos apsaugos ministerija, Sistemos tvarkytojas yra RC.

2.2. Sistemos naudotojai ir tikslinės grupės

44. Sistemos naudotojų aprašymas pateiktas 2-oje lentelėje.

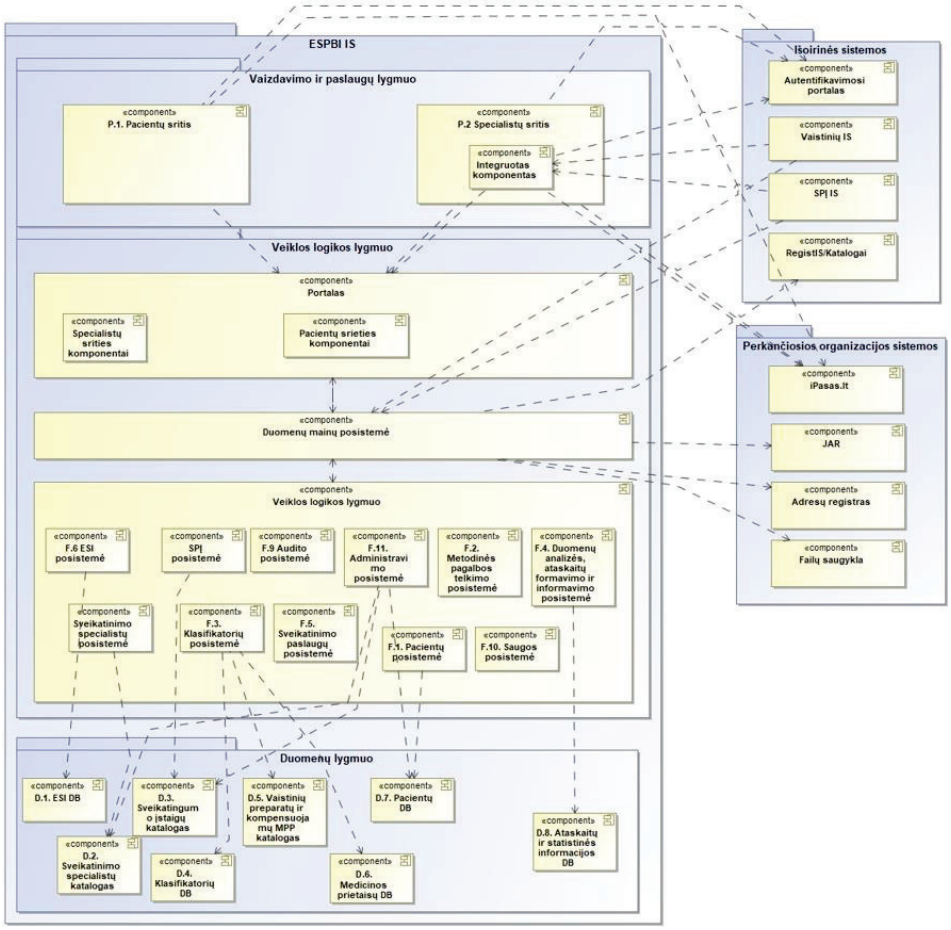
2 lentelė. Sistemos naudotojų aprašymas

Nr.	Naudotojas	Aprašymas
1.	Pacientas	Asmuo, kuris naudojasi sveikatos priežiūros įstaigų teikiamomis paslaugomis, nepaisant to, ar jis sveikas ar ligonis.
2.	Sveikatos priežiūros specialistas	Asmuo, teikiantis sveikatos priežiūros paslaugas – Šeimos gydytojas, ar bet kurios kitos specializacijos gydytojas (išskyrus radiologinius, ultragarsinius, EKG ir EEG tyrimus diagnozuojančius gydytojus specialistus), galintis peržiūrėti paciento sveikatos istoriją, rengti tyrimų užsakymus. Ši rolė nesuteikia teisės rengti medicininių vaizdų diagnostinių aprašymų.
3.	Radiologas	Gydytojas radiologas peržiūrintis įrenginių sukurtus medicininius radiologinius vaizdus, darantis medicininių vaizdų anotacijas, sukuriantis tyrimų diagnostinius aprašymus ir turintis teisę juos pasirašyti. Ultragarsinių, EKG ir EEG tyrimų diagnozavimo atveju sąvoka –Radiologas – nagrinėjant PA sąlygiškai praplečiama ir apima kitus gydytojus specialistus, turinčius teisę diagnozuoti atitinkamus tyrimus.
4.	PACS	Su MedVAIS saugiu ryšiu sujungta SPĮ PACS, teikianti ar gaunanti medicininius vaizdus.
5.	HIS	Su ESPBI IS sujungta sveikatos priežiūros įstaigos informacinė sistema.
6.	RIS	Su ESPBI IS sujungta sveikatos priežiūros įstaigos radiologinio padalinio informacinė sistema.

Nr.	Naudotojas	Aprašymas
7.	Sveikatos priežiūros veiklą koordinuojančios ir administruojančios organizacijos	Sveikatos priežiūros veiklą koordinuojančios ir administruojančios organizacijos, kurioms MedVAIS duomenys reikalingi sveikatos apsaugos politikos formavimui.
8.	Mokslinę veiklą vykdančios organizacijos	Mokslinę veikla vykdančios organizacijos, kurioms MedVAIS duomenys reikalingi mokslinių tyrimų tikslams.

2.3. Sistemos funkcinė struktūra architektūrai

45. ESPBI IS nuostatų IV punkte nurodyti ESPBI IS funkciniai komponentai sudaro funkcinę architektūrą ir aprašomi ESPBI IS loginiame modelyje.
46. ESPBI IS yra pagrindinė skaitmeninės sveikatos sistemos įgyvendinimo priemonė – Lietuvos Respublikos sveikatos sistemos organizacinių, telekomunikacinių ir programinių priemonių bei duomenų bazių, skirtų elektroninės asmens sveikatos istorijoms centralizuotai formuoti, naudoti ir kaupti bei jomis keistis tarp sveikatinimo veiklą vykdančių įstaigų, jų specialistų ir kitų darbuotojų, visuma. ESPBI IS užtikrina Lietuvos skaitmeninės sveikatos sistemos subjektų bendradarbiavimą ir jų informacinių sistemų integraciją per duomenų mainų posistemę, skaitmeninės sveikatos paslaugų veikimą ir prieigą prie viešojo administravimo institucijų informacinių išteklių.



3 pav. Skaitmeninės sveikatos sistemos architektūros schema

2.3.1. Sistemos loginis modelis

47. ESPBI IS posistemės:

- Pacientų ir sveikatinimo specialistų prieigos prie e. paslaugų posistemė – Skaitmeninės sveikatos portalas (toliau – Portalas) – kompiuterinių priemonių, skirtų vieno langelio prieigos gyventojams bei sveikatos priežiūros ir farmacijos specialistams principui įgyvendinti, visuma.
- Autentiškumo užtikrinimo posistemė – VIISP priemonėmis ar tiesioginėmis ESPBI IS naudotojų identifikavimo priemonėmis užtikrina ESPBI IS naudotojų tapatybės nustatymą, Portalo naudotojų tapatybės nustatymą, generuoja elektroninį spaudą ir leidžia pasirašyti elektronines dokumentų formas elektroniniu spaudu. Visų ESPBI IS naudotojų autentifikavimas vykdomas per VIISP naudotojų tapatybės nustatymo modulį.
- Administravimo posistemė – užtikrina ESPBI IS valdymą, efektyvias ESPBI IS administravimo priemones ir ESPBI IS vykstančių techninių (sisteminių) procesų stebėjimą.
- Saugos posistemė – registruoja ESPBI IS naudotojus, suteikia ir tvarko ESPBI IS naudotojų prieigos prie duomenų teises, užtikrina ESPBI IS naudotojų tapatybės nustatymą ir Portalo naudotojų tapatybės nustatymą, pasitelkiant VIISP priemones, užtikrina ESPBI IS naudotojų teisių valdymą, užtikrina ESPBI IS duomenų saugą, užtikrina ESPBI IS duomenų archyvavimą ir rezervinių duomenų kopijų darymą.
- Audito posistemė – užtikrina efektyvias ESPBI IS stebėsenos ir audito priemones, registruoja visus ESPBI IS naudotojų veiksmus, užtikrina audito įrašų vientisumą ir įrašų paiešką, rengia ESPBI IS naudotojų veiksmų ataskaitas.
- ESI posistemė – užtikrina ESI duomenų tvarkymą ir paiešką, paciento duomenų teikimą ESPBI IS duomenų mainų ir Portalo posistemėms.
- Pacientų posistemė – užtikrina pacientų bendrųjų duomenų tvarkymą ir paiešką, paciento identifikavimą pagal jo vardą, pavardę ir gimimo datą, asmens kodą, lytį, ESI identifikacinį numerį.
- Klasifikatorių posistemė centralizuotai tvarko klasifikatorių duomenis, teikia klasifikatorių duomenis ESPBI IS tvarkytojams, ESPBI IS duomenų teikėjams ir kitoms suinteresuotoms institucijoms, užtikrina klasifikatorių duomenų paiešką.
- E. recepto posistemė – sudaro sąlygas išrašyti vaistinius preparatus ir kompensuojamąsias medicinos pagalbos priemones elektroniniu būdu ir kaupia duomenis apie juos, tvarko elektroniniu būdu išrašytų receptų duomenis, rengia ir teikia išrašytų vaistinių preparatų ir kompensuojamųjų medicinos pagalbos priemonių ataskaitas, užtikrina e. receptų duomenų paiešką.
- Medicininių vaizdų posistemė – užtikrina nacionalinės medicininių vaizdų saugyklos veikimą, tvarko medicininius vaizdus, užtikrina sveikatos priežiūros specialistams ir pacientams prieigą prie saugomų medicininių vaizdų ir medicininių vaizdų paiešką.
- Sveikatinimo paslaugų posistemė – kaupia ir teikia duomenis apie suteiktas sveikatinimo paslaugas, rengia ir teikia suteiktų sveikatinimo paslaugų, kompensuojamų iš Privalomojo sveikatos draudimo fondo biudžeto, ataskaitas.
- Metodinės pagalbos teikimo sveikatinimo specialistui posistemė – teikia informaciją apie rekomenduojamus tyrimo, gydymo būdus, teikia vaistinių preparatų klinikinę informaciją ir kitą metodinę informaciją.
- Duomenų analizės, ataskaitų formavimo ir informavimo posistemė – teikia ataskaitas pagal iš anksto nustatytus rodiklius, užtikrina duomenų analizės įvairiais pjūviais, naudojant programines analizės priemones, vykdymą, užtikrina ligų ir sergamumo analizės bei ataskaitų rengimą, rengia ir teikia statistines ir visuomenės sveikatos stebėsenos ataskaitas ir kitas

sveikatinimo veiklos valdymo subjektams reikalingas ataskaitas, formuoja statistines ir analitines ataskaitas iš kitų posistemių duomenų, teikia visuomenei viešą statistinę informaciją.

- Nėščiųjų, gimdyvių ir naujagimių posistemė – registruoja nėščiąsias, gimdyves ir naujagimius ir vykdo jų paiešką, kaupia ir saugo klinikinę informaciją apie nėščiąsias, gimdyves ir naujagimius, atlieka duomenų statistinę analizę ir formuoja ataskaitas, vykdo duomenų mainus su kitomis informacinėmis sistemomis, valdo naudotojų teises ir roles, nėščiųjų, gimdyvių ir naujagimių informacinės sistemos parametrus, taip pat saugo naudotojų ir jų prisijungimo duomenis, dokumentus ir jų šablonus.
- Slaugos paslaugų posistemė – kaupia ir saugo duomenis apie asmens slaugą, sudaro galimybę slaugytojui fiksuoti visą su slauga susijusią informaciją elektroninių dokumentų formose, leidžia slaugos paslaugas pateikti Portale arba per tinklines sąsajas – ESPBI IS slaugos posistemėje užfiksuoti slaugos procedūrų ir tyrimų iš mobiliųjų įrenginių duomenis ir atvaizduoti pacientams arba jų įgaliotiems asmenims Portale.
- Duomenų mainų posistemė – užtikrina duomenų mainus tarp ESPBI IS ir kitų skaitmeninės sveikatos sistemos komponentų (sveikatinimo veiklą vykdančių įstaigų informacinių sistemų, sveikatos sektoriaus registrų ir informacinių sistemų ir kitų viešojo administravimo sektorių), elektroninės medicininės istorijos (EMI) duomenų mainus tarp Mobiliosios programėlės ir kitų duomenų mainų komponentų, taip pat teikia ESPBI IS klasifikatorių duomenis sveikatinimo įstaigų ir suinteresuotų institucijų informacinėms sistemoms.

48. MedVAIS posistemė:

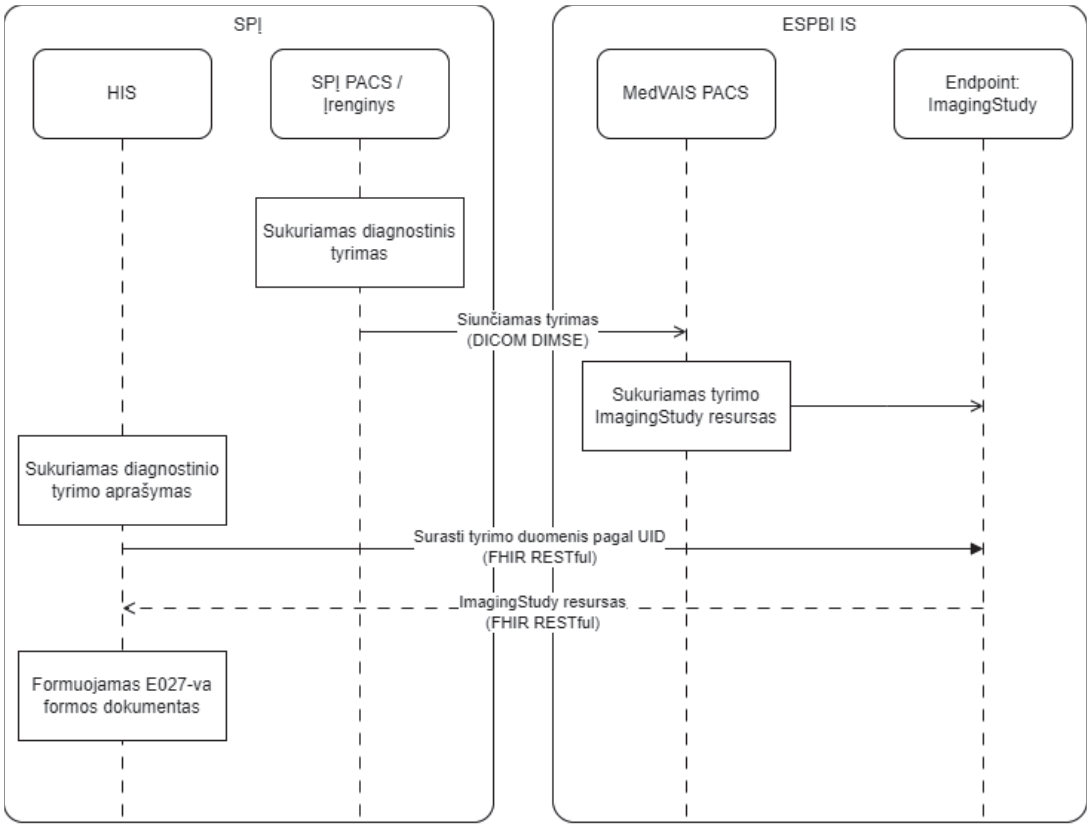
- MedVAIS architektūra paremta virtualių PACS sistemų sukūrimu kiekvienai medicininius vaizdus į MedVAIS siunčiančiai ar iš MedVAIS MV gaunančiai ASPĮ. PACS sistemos sukuriamos atskirose virtualiose mašinose kaip DCM4CHEE 4.3.0 egzempliorius.
- DCM4CHEE karkaso veikimas paremtas principu vienas DCM4CHEE egzempliorius – viena įstaiga. Dėl to, kiekvienai įstaigai sukuriama atskira duomenų bazės schema, kurioje visus saugomus duomenis PACS traktuoja kaip tik tos įtaigos duomenis. Yra tiek savo struktūra identiškų duomenų bazių schemų, kiek sukuriama virtualių PACS prieigų įstaigoms.
- Ryšio tarp ASPĮ PACS ir MedVAIS PACS sistemos palaikymui naudojamas saugus VPN kanalas.
- Duomenų modelis ir funkcionalumai MedVAIS posistemėje susideda iš dviejų loginių sričių: MedVAIS PACS duomenų struktūros ir funkcionalumų srities bei ESPBI IS MedVAIS duomenų struktūros ir funkcionalumų srities.
- MedVAIS PACS duomenų struktūros ir funkcionalumų sritis apima sistemos veikimo dalį, kurioje realizuotos virtualios PACS sistemos, skirtos darbui su SPĮ Įrenginiais bei užtikrina DICOM komunikaciją. Šioje dalyje kaupiami duomenys, kurie sistemoje atsiranda komunikacijos DICOM protokolu metu, bei papildomi ir pagalbiniai duomenys.
- ESPBI IS MedVAIS duomenų struktūros ir funkcionalumų sritis apima visas duomenų struktūras, kurios realizuojamos ESPBI IS dalyje. Kadangi E. sveikatos portalo atžvilgiu MedVAIS yra kaip integrali, vieninga ESPBI IS posistemė, su Portalo veikimu susiję MedVAIS komponentai realizuojami tomis pačiomis priemonėmis ir principais kaip ESPBI IS centrinė dalis, kartu įgyvendinant ir vieningą duomenų modelį. Todėl medicininio vaizdo diagnostinio aprašymo ir medicininio vaizdo esybės realizuojamos kaip FHIR standarto resursai. Taikomi ir tie patys duomenų valdymo principai – E027-va el. dokumentas konstruojamas kaip FHIR resursų kompozicija, resursų duomenys saugomi toje pačioje duomenų bazės schemoje greta

ESPBI IS centrinės dalies resursų duomenų lentelių, resursų nuorodos nukreipia į ESPBI IS centrinės dalies valdomus resursus (paciento, gydytojo, įstaigos resursai). Duomenų sąsaja tarp dviejų dalių realizuojama per tyrimo esybę. Atsiunčiamas diagnostinis tyrimas visada turi unikalų UID, kuris registruojamas tiek DCM4CHEE schemos lentelėje, tiek atitinkamame FHIR resurse. FHIR resurse ImagingStudy registruojami ir kiti DICOM duomenys, tačiau tyrimo UID lieka pagrindine sąsaja tarp abejose srityse esančių duomenų struktūrų.

Integracija su MedVAIS paremta architektūriniu principu, kad naudojami du pagrindiniai komunikacijos su MedVAIS kanalai:

- Medicininiams vaizdams teikti ir gauti – DICOM komunikacija su MedVAIS PACS. Visa komunikacija ir duomenų apsikeitimas tarp SPĮ PACS / Įrenginių ir MedVAIS PACS vykdoma pagal DICOM 3.0 standarto protokolą.
- Aprašomiesiems ir kitiems susijusiems medicininiams duomenims ir dokumentams – FHIR komunikacija per ESPBI IS integracinius taškus.

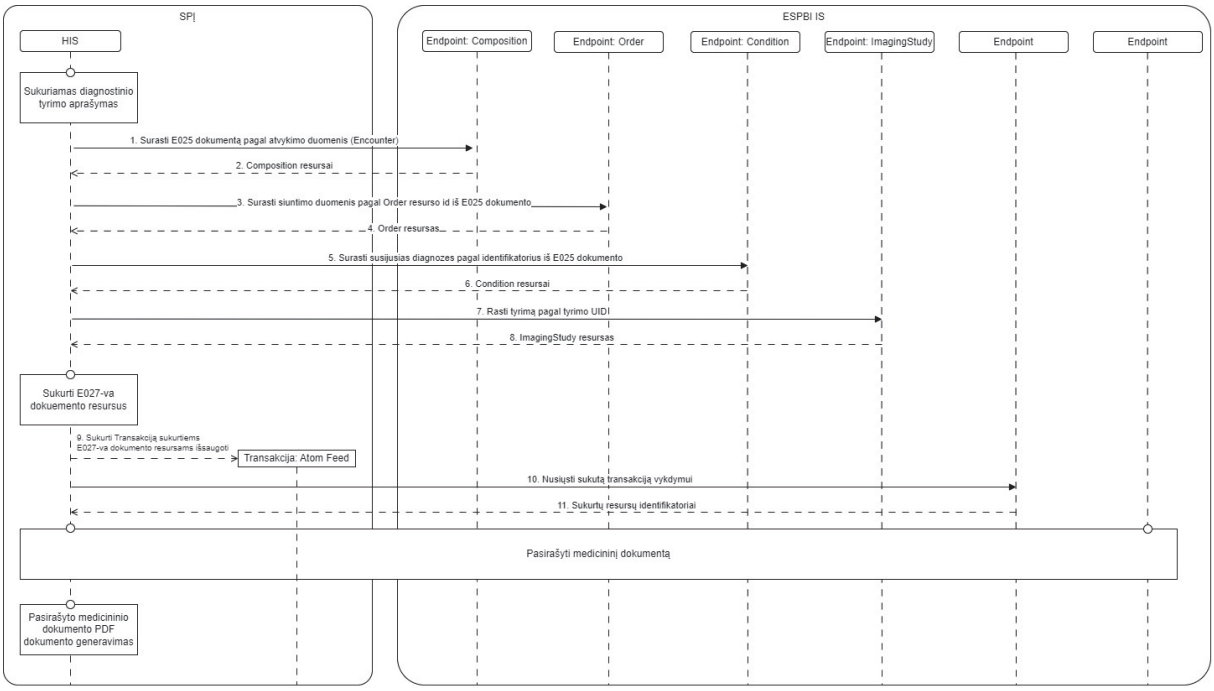
Kiekvienam medicininiam vaizdui, kuris pateikiamas DICOM protokolu į MedVAIS, MedVAIS sukuriamas tyrimo FHIR resursas – ImagingStudy. Visiems tolimesniems veiksmams tiek per E. Sveikatos portalą, tiek per integraciją su SPĮ IS, kai reikalinga surasti, aprašyti, peržiūrėti ar kitaip valdyti diagnostinį tyrimą, naudojamas atitinkamas ImagingStudy resursas. Resurso atitiktį su konkrečiu diagnostiniu tyrimu visais atvejais nusako unikalus tyrimo identifikatorius (UID). Žemiau pateikiama pavyzdinė integracijos schema diagnostinio tyrimo aprašymo rengimo atveju.



4 pav. Pavyzdinė integracijos schema diagnostinio resurso tyrimo aprašymo rengimo atveju

E027-va. diagnostinio tyrimo aprašymas dokumento pateikimas yra realizuotas sąveikos scenarijumi pateiktu paveiksle žemiau. Medicininio tyrimo aprašymas FHIR RESTful protokolu perduodamas į

aktualius integracinius taškus kaip pateikta pavyzdyje. Pavyzdyje pateiktame pasirašymo komponente yra generuojamas, pasirašomas ir saugomas PDF dokumentas, atitinkantis medicininio vaizdo aprašymo duomenų rinkinį pateiktą 3-ioje lentelėje kartu su įstaigos, paciento ir specialisto duomenimis.



5 pav. E027-va. diagnostinio tyrimo aprašymas dokumento pateikimas realizavimo sąveikos scenarijus

Įstaigų integracija ir sąveika su MedVAIS detaliau pateikta ESPBI IS duomenų mainų ir integracijos projektavimo dokumentacijoje, 3.15 skyriuje „SPĮ ir MedVAIS integracijos dokumentacija“[1].

3 lentelė. Medicininio vaizdo aprašymo formos duomenų rinkinys

Nr.	Formos laukas	FHIR resursas	Resurso atributas
10.1.	**Siuntimo duomenys:**		
10.1.1.	Atvyko su siuntimu (TAIP / NE):	Encounter	type: CodeableConcept [0..*]
10.1.1.1.	Nuoroda į siuntimo el. dokumentą		indication: Order [0..1]
10.1.1.2.	Siuntimo numeris	Order	id: identifier [1]
10.1.1.3.	Siuntimo data ir laikas	Order	date: dateTime [0..1]
10.1.1.4.	Siuntimo diagnozė	Condition	text : String [0..1]
10.1.1.5.	Siuntimo diagnozės kodas	Condition	code : String [0..1]
10.1.2.	Atvyko be siuntimo (žyma)		
10.2.	**Tyrimo aprašymo informacija:**		
10.2.1.	Tyrimo (medicininio vaizdo) aprašymo numeris	DocumentReference	masterIdentifier: String [1]
10.2.2.	Tyrimo UID	ImagingStudy	uid: String [1]
10.2.3.	Tyrimo data ir laikas	ImagingStudy	dateTime: dateTime [1]
10.2.4.	Tyrimo pavadinimas	ImagingStudy	description: String [0..1]
10.2.5.	Tyrimo ACHI kodas	DiagnosticReport	name: codeableConcept [1]
10.2.6.	Pacientas neidentifikuotas (žyma)	Patient	identifier : codeableConcept [1]
10.2.7.	Prisegta (-os) byla (-os) (TAIP / NE):	List	entry: Image [0..*]
10.2.7.1.	Bylų skaičius	List	entry: Image [0..*]
10.3.	Tyrimo (medicininio vaizdo) aprašas	DiagnosticReport	description: String [1]
10.4.	Išvada	DiagnosticReport	conclusion: String [1]

[1] https://www.esveikata.lt/espbi-specifikacija

10.5.	**Pagrindinė diagnozė:**		
10.5.1.	TLK-10-AM kodas	Condition	code: CoadeableConcept [1]
10.5.2.	Pavadinimas	Condition	display: String [1]
10.5.3.	Aprašymas	Condition	notes: String [0..1]
10.6.	Diagnozė 1		
10.7.	Diagnozė 2		
10.8.	**Jonizuojančios spinduliuotės duomenys:**		
10.8.1.	Įrenginio serijinis numeris	Observation	valueString: String [0..1]
10.8.2.	Dozė	Observation	valueQuantity: Quantity [0..1]
10.8.3.	Matavimo vienetas	Observation	valueQuantity: String [0..1]
10.9.	**Susiję tyrimai:**		
10.9.1.	Pavadinimas	ImagingStudy	description: text [1]
10.9.2.	Susijusio tyrimo numeris	ImagingStudy	uid : String [0..1]

2.3.2. Naudojamos technologijos

49. Oracle EE;
50. Java;
51. Angular;
52. TypeScript;
53. RabbitMQ;
54. Flutter;
55. CentOS, Red Hat Fuse;
56. Power BI;
57. WildFly;
58. DCM4CHE.

2.4. Sistemos fizinė struktūra

59. MedVAIS failinės saugyklos duomenų saugojimas užtikrinamas naudojant 2 komplektus saugojimo sistemų, kur kiekvienoje iš jų yra:

59.1 Xcellis MDC duomenų prieigos valdikliai – sukuria vieningą failinę sistemą bei pateikia aukšto našumo (HA) duomenų prieigą prie failinės sistemos. Taip pat, užtikrina failinės sistemos duomenų kopijavimą be papildomo vartotojo įsikišimo (transparent data management);

59.2 Quantum QXS424 duomenų saugykla – aukšto našumo saugykla, kurioje saugomi failinės sistemos meta duomenys;

59.3 Bull Optima3700 duomenų saugykla – saugomi failinės sistemos duomenys;

59.4 Quantum QXS584 duomenų saugykla – saugomi failinės sistemos duomenys;

59.5 Quantum AEL500 juostų biblioteka – pagal nustatytą politiką į šią biblioteką Xcellis MDC gali perkelti duomenis iš duomenų saugyklų be papildomo vartotojo įsikišimo. Vartotojui prireikus duomenų – jie automatiškai atstatomi į duomenų saugyklą.

59.6 Xcellis Workflow Extender – valdiklis, atsakingas už duomenų replikavimą tarp pagrindinės ir rezervinės saugojimo sistemos;

59.7 Quantum QXS584 kartu su Bull Optima 3700 sudaro pagrindinę medicininių vaizdų talpą, iš kurios šiuo metu yra užimta 1,4 PB.

3. SISTEMOS PAGEIDAUJAMOS BŪSENOS APRAŠYMAS

60. Šios Paslaugų teikimo sutarties apimtyje siekiama modernizuoti ir įdiegti Sistemą, kuri realizuotų šias naujas funkcijas:

60.1. **Medicininių vaizdų prieiga** – funkcionalumas leidžiantis sveikatos priežiūros specialistui pasiekti ir atsisiųsti pacientų medicininius tyrimus ir jų aprašymus iš skirtingų, tyrimus į MedVAIS pateikusių, įstaigų:

60.1.1. Sudaryta galimybė teikti pacientui atliktų tyrimų sąrašo užklausą DICOM protokolu;

60.1.2. Sudaryta galimybė atsisiųsti medicininius vaizdus pagal pateiktą sąrašą DICOM DIMSE servisais;

60.1.3. Sudaryta galimybė atsisiųsti medicininius vaizdus DICOMweb servisais;

60.1.4. MedVAIS, pasinaudodamas ESPBI IS naudotojų prieigos teisių mechanizmu gali patikrinti ar ASPĮ ir konkretus gydytojas turi prieigos prie paciento duomenų teisę.

60.2. **Medicininių tyrimų peržiūros įrankis** – medicininių vaizdų (DICOM ir ne DICOM formato) peržiūros įrankis, kurio prieinamumas vartotojui valdomas pagal jo rolę. Funkcionalumas turi būti pritaikytas vartotojo darbui HIS aplinkoje ir e. sveikatos portaluose bei nereikalaujantis jokių diegimo vartotojo kompiuteryje veiksmų.

60.3. **Ne DICOM formato failų perdavimo galimybė** – funkcionalumas leidžiantis MedVAIS priimti ir saugoti ne DICOM standartu perduodamas rinkmenas, su tikslu jas atidaryti tame pačiame medicininių vaizdų peržiūros įrankyje bei galimybe dalintis tarp įstaigų DICOM standarto protokolais. Funkcionalumas turi būti pritaikytas vartotojo darbui HIS aplinkoje ir e. sveikatos portaluose.

60.4. **Duomenų registro ir duomenų saugyklos valdymo funkcionalumas** – modernizuojamas MedVAIS turi turėti duomenų registro ir saugyklos valdymo funkcionalumą, leidžiantį:

60.4.1. Migruoti duomenis iš esamo PACS į modernizuojamą sistemą;

60.4.2. Migruoti duomenis esamoje infrastruktūroje, tais atvejais kai neišvengiamai reikia atnaujinti jos komponentus;

60.5. **Hibridinio modelio įgalinimas** – po šio paslaugos pirkimo įgyvendinimo MedVAIS atliks centrinio registro ir saugyklos funkcijas. Tačiau, modernizuojama sistema taip pat turi užtikrinti galimybę ateityje pritaikyti hibridinį duomenų saugojimo modelį Lietuvoje:

60.5.1. Hibridinio modelio atveju, medicininių vaizdų saugyklų funkciją atliktų ne tik MedVAIS, tačiau ir ASPĮ, turinčios tam reikiamą infrastruktūrą.

60.5.2. MedVAIS atliktų pagrindinio registro bei vienos iš medicininių vaizdų saugyklų funkcijas.

60.5.3. Hibridinio modeliu atveju ASPĮ galėtų pasirinkti teikti į MedVAIS medicininį vaizdą saugojimui arba teikti informaciją apie medicininį vaizdą su galimybe jį atsisiųsti kitoms ASPĮ.

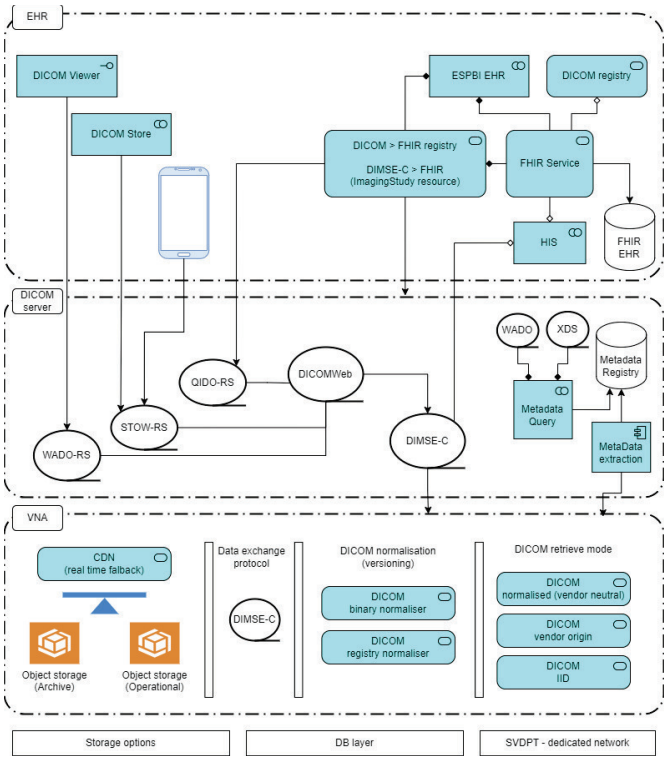
60.5.4. ASPĮ kreipdamasi į MedVAIS atsisiųstų tyrimą iš MedVAIS arba gautų nuorodą iš ASPĮ, kurioje saugomas tyrimas.

60.6. **Medicininio tyrimo nuasmeninimo funkcionalumas** – modernizuojamas MedVAIS turi galėti nuasmeninti medicininius vaizdus (metaduomenis ir pikseliuose išsaugotą informaciją (angl. burned into pixel data)) pakartotiniam panaudojimui.

60.7. **Duomenų gyvavimo ciklo valdymo funkcionalumas** – atnaujinta MedVAIS sistema turi galėti taikyti medicininių vaizdų, kitų DICOM ir ne DICOM formato rinkmenų gyvavimo ciklo valdymo taisykles, nustatančias saugojimo atminties erdvių naudojimą. Turi būti galimybė valdyti duomenų saugojimą skirtingose atminties erdvėse pagal su paciento duomenimis susijusius ir kitus įvykius (pvz.: užregistruotas apsilankymas).

Siekiamus įgyvendinti funkcionalumus atspindi pirminė sistemos protokolus ir sudedamąsias dalis apibendrinanti schema (žr. 6 pav.):

- VNA – (angl. Vendor neutral archive) atliekamas duomenų valdymas tarp atminties sričių ir užtikrintas duomenų priėmimas ir atidavimas nepriklausomai nuo duomenų teikėjo pradinio ir pageidaujamo formatų (normalizuoti metaduomenys ir rinkmena).
- DICOM serveris – įgyvendinti DICOM standarto protokolai (DIMSE ir DICOMWeb) duomenų perdavimui ir peržiūros įrankio prieigai bei tyrimų metaduomenų valdymas.
- EHR – medicininių vaizdų duomenų ir elektroninės sveikatos istorijos registro sąsaja bei vartotojų komponentai tiesiogiai naudojantys DICOM protokolus (WADO-RS – medicininių vaizdų perdavimas, STOW-RS – medicininių vaizdų saugojimas, DIMSE – duomenų apsikeitimas tarp sistemos ir vaizdus generuojančių įrenginių bei kitų aplikacijų ar sistemų palaikančių DIMSE protokolus).
- Infrastruktūros, duomenų bazės ir tinklų dedamosios detalizuojamos projekto įgyvendinimo metu.



6 pav. Numatomų architektūros komponentų schema

4. FUNKCINIŲ REIKALAVIMŲ APRAŠYMAS

61. Šiame skyriuje pateikti funkciniai reikalavimai, kuriuos Teikėjas turės patikslinti ir suderinti su Perkančiosios organizacijos (toliau – Perkančioji organizacija, Registrų centras, RC) atstovais detalios analizės ir projektavimo etapų metu. Esant poreikiui, funkciniai reikalavimai gali būti pakoreguoti, bet tik suderinus ir patvirtinus keitimus su Perkančiąja organizacija. Priėmimo testavimo metu Teikėjas privalės pademonstruoti visus toliau išvardytus funkcinius reikalavimus.

4.1. Bendrieji reikalavimai

Reikalavimo Nr.	Aprašymas
BR_1.	Kurdamas visas pageidaujamas projekto funkcijas Teikėjas turi vadovautis šioje techninėje specifikacijoje pateikiamais reikalavimais bei specifikacijos priedais.
BR_2.	Kūrimo metu turi būti išlaikyti ir nesugadinti visi šiuo metu ESPBI IS esantys funkcionalumai.
BR_3.	Teikėjas turės bendradarbiauti su paraleliai vykdomų ESPBI IS modernizavimo veiklų paslaugų teikėjais.
BR_4.	Projekto įgyvendinimo metu turi būti griežtai atsižvelgta į ESPBI IS: 1. Naudojamas technologijas; 2. Naudojamą standartinę programinę įrangą; 3. Duomenų modelio architektūra; 4. Tarnybinių stočių, kompiuterinio tinklo bei jame naudojamų įrenginių architektūra; 5. Vidines ir išorines integracijas bei duomenų srautus; 6. Naudojamas duomenų klasifikacijas; 7. Naudotojų identifikacijos ir prieigos teisių modelį; 8. Automatizuotus veiklos procesus.
BR_5.	MedVAIS funkcijos turi būti kuriamos kaip integrali ESPBI IS dalis, sveikatos priežiūros paslaugų teikimui panaudojant esamas ESPBI IS priemones bei sukuriant trūkstamas.
BR_6.	Realizuojant turi būti perpanaudotos standartinės ESPBI IS funkcijos ir komponentai, pvz: 1. Posistemėje vykdomų veiksmų auditavimui; 2. Dokumentų valdymui (kūrimui, ruošinių naudojimui ir pan.) 3. Funkcijoms susijusioms su komunikacija (pranešimų siuntimas, priminimų teikimas ir pan.); 4. Funkcijoms susijusioms su kalendoriumi; 5. Duomenų analizei, ataskaitų formavimui; 6. Administravimui ir kitoms funkcijoms. Teikėjas turės pateikti reikalavimus standartinių ESPBI IS komponentų pakeitimams, kurie bus reikalingi realizuojant projektą ir su ją susijusius veiklos procesus.
BR_7.	Sukurtos duomenų įvedimo formos turi būti konstruojamos taip, kad duomenų įvedimas būtų kiek įmanoma labiau struktūrizuotas.
BR_8.	Realizuojant projekto funkcinius ir nefunkcinius reikalavimus turi būti atitinkamai modifikuojamos ir ESPBI IS administravimo priemonės, leisiančios tinkamai administruoti sukurtus funkcionalumus.
BR_9.	Duomenų įvedimo formos turi būti kiek įmanoma automatizuotai užpildomos duomenimis, kurie jau yra saugomi ESPBI IS ar kitose per integracines sąsajas pasiekiamose IS ir registruose. Teikėjas detalios analizės ir projektavimo etapų metu turi nustatyti ir su Perkančiąją organizacija suderinti kurie formų duomenys bus automatiškai užpildomi numatytomis reikšmėmis.
BR_10.	Projekto sąrašuose turi būti realizuotas: 1. Puslapiavimas;

	2. Sąrašuose turi būti atvaizduojamas įrašų sąraše skaičius. Atlikus sąrašo filtravimą turi būti vaizduojamas rastų įrašų skaičius. 3. Turi būti galima sąrašą filtruoti ir rūšiuoti pagal tam sąrašui priklausančius atributus. Išimtys gali būti taikomos suderinus sprendimą su Perkančiąją organizacija.
BR_11.	Visos paieškos / filtravimo funkcijos, išskyrus atvejus, kuriuos Teikėjas suderins detalios analizės ir projektavimo etapo metu, turi būti realizuotos pagal šias taisykles: 1. Tekstiniuose paieškos laukuose turi būti realizuota paieška pagal žodžio ar skaičių junginio fragmentą ir pilną žodį; 2. Paieška turi būti atliekama pagal lietuviškas raides ir vietoje lietuviškų raidžių naudojant lotyniškus raidžių atitikmenis (pavyzdžiui „š“ ir „s“ raides traktuojant kaip vieną); 3. Paieška turi būti vykdoma neatsižvelgiant į didžiąsias ir mažąsias raides; 4. Paieška turi būti vykdoma tik tuose komponentuose ir duomenų aibėje, prie kurių naudotojas turi prieigos teises; 5. Paieškos rezultatai turi būti pateikiami sąrašo forma; 6. Atlikus paiešką, turi būti rodomas paieškos rezultatų skaičius.
BR_12.	Turi būti vykdomas į duomenų įvedimo formas įvedamų duomenų tikrinimas (ang. Validation) pagal detalios analizės ir projektavimo metu formoms nustatytas tikrinimo taisykles: 1. Turi būti tikrinami privalomi įvesti duomenys; 2. Turi būti tikrinamas duomenų formatas (datos, skaičiaus, teksto ar kitas nustatytas taisykles); 3. Turi būti tikrinami pridedamų rinkmenų plėtiniai ir rinkmenos dydis; 4. Turi būti atliekamas loginis tikrinimas tarp formos elementų - vieno formos elemento parinkimas (įvedimas) turi galėti įjungti / išjungti kitus formos elementus ir pan.
BR_13.	Visoms šioje techninėje specifikacijoje aprašytoms funkcijoms, kurių metu yra sukuriami duomenys ar dokumentai, turi būti realizuojamos tų duomenų ar dokumentų redagavimo bei šalinimo ar anuliavimo funkcijos, kurios turi būti suderintos su veiklos logika.
BR_14.	Projektu metu realizuotos ar pakeistos duomenų rinkinių valdymo taisyklės turi būti tokios pačios kaip visoje ESPBI IS.
BR_15.	Projekto metu realizuojamos formos turi atitikti visus bendrus ESPBI IS formoms keliamus reikalavimus ir būti realizuotos vieningais principais.
BR_16.	Prieiga prie funkcionalumo ir duomenų pasiekiamumas turi būti valdomas per bendrą ESPBI IS teisių prieigos mechanizmą.
BR_17.	Projekto metu realizuotos dokumentų rinkinių pasirašymo taisyklės turi būti tokios pačios kaip ESPBI IS.
BR_18.	Naudotojai turi galėti jungtis iš bet kurio suderinamo įrenginio (pvz., kompiuterio, išmaniojo telefono, planšetės).
BR_19.	Detalios analizės ir projektavimo metu Teikėjas su Perkančiąją organizacija turi susiderinti įgalioto, pavaduojančio specialisto, paciento atstovo, specialių naudotojų turimas teises naujai realizuotų funkcijų apimtyje ir papildyti arba

	sukurti reikalingus klasifikatorius (sisteminių pranešimų, įgaliojimų tipų klasifikatorių ir t.t.).
BR_20.	Naudotojai savo asmeninėje paskyroje turi turėti galimybę nustatyti informavimo galimybę pagal savo rolę. Tokia ESPBI IS funkcija yra, tačiau reikia pritaikyti prie naujų, projekto apimtyje atsirandančių, pranešimų.
BR_21.	Bendrų registrų (klasifikatorių) duomenys Sistemoje turi būti įvedami vieną kartą, t.y., negali būti dubliuojami nei vieno registro duomenys.
BR_22.	Vystant Sistemą Teikėjas turi įvertinti BDAR keliamus reikalavimus, suprojektuoti Sistemos duomenų modelį ir įgyvendinti duomenų subjektų teisių įgyvendinimo sprendimus, siekiant sudaryti galimybes įgyvendinti duomenų subjektų, kurių duomenys tvarkomi Sistemos priemonėmis, teises.
BR_23.	Turi būti aktualizuota naudotojams skirta informacija apie Sistemą ir jame atliekamą asmens duomenų tvarkymą, duomenų subjektų teises ir jų įgyvendinimą.
BR_24.	Vystymo metu Sistema turi būti sukonfigūruota taip, kad pagal nutylėjimą sisteminiai parametrai užtikrintų didžiausią asmens duomenų apsaugą (angl. Privacy by default).

4.2. Funkciniai reikalavimai Sistemai

Funkciniai reikalavimai, susiję su medicininių vaizdų prieiga:

Reikalavimo Nr.	Aprašymas
FR_1.	Turi būti sudaryta galimybė teikti medicininių vaizdų sąrašo užklausą DICOM protokolu (C-FIND, QIDO-RS).
FR_2.	Sudaryta galimybė atsisiųsti medicininius vaizdus pagal pateiktą sąrašą DICOM protokolu (C-MOVE, WADO-RS);
FR_3.	MedVAIS turi gebėti pasitikrinti ar savo saugykloje turi diagnostinį tyrimą pagal nurodytus užklausos parametrus ir pateikti tyrimo duomenų būklės požymį(-ius).
FR_4.	MedVAIS turi gebėti pasitikrinti, panaudodama ESPBI IS naudotojų teisių mechanizmą, ar užklausą pateikusi SPĮ ir konkretus Specialistas turi prieigos prie Paciento ESI teisę.
FR_5.	MedVAIS turi gebėti nusiųsti pranešimą, nurodantį užklausos neįvykdymo priežastį(-is) pateiktais atvejais (tačiau neapsiribojant tik pateiktais): kuomet prieiga prie Paciento ESI neleidžiama, MedVAIS užsakyto diagnostinio tyrimo neturi ir kitais atvejais suderintais detalios Analizės etape.
FR_6.	MedVAIS turi gebėti pagal užklausoje (DICOM DIMSE ir DICOMweb) pateiktus parametrus iš DICOM duomenų bazės išrinkti visus Paciento diagnostinius tyrimus, kuriems yra priskirtas Pacientas, ir suformuoti diagnostinių tyrimų sąrašą.
FR_7.	MedVAIS turi gebėti perduoti DICOM DIMSE ir DICOMweb protokolais gautoje užklausoje nurodytus diagnostinių tyrimų duomenis atsižvelgiant į tai ar gautoje užklausoje prašoma teikti originalius, subendrintus (angl. vendor neutral) tyrimų duomenis ar kitus elementus, kuriuos leidžia teikti WADO-RS technologija.

FR_8.	MedVAIS Administratoriui turi būti sudaryta prieiga prie su Funkcionalumo veikimu bei naudojimu susijusios IS sisteminių žurnalų įrašų informacijos ir suteiktos priemonės ją analizuoti. Teikėjo siūlomi sprendiniai ir priemonės turi būti suderinti su Perkančiąja organizacija Analizės etape.
FR_9.	Turi būti sukurta su Funkcionalumo veikimu bei naudojimu susijusios informacijos daugiaparametrinės paieškos IS sisteminiuose žurnaluose funkcija. Teikėjo siūlomi sprendiniai ir priemonės turi būti suderinti su RC. Teikėjas turi atsižvelgti į RC siūlymus.
FR_10.	MedVAIS Administratoriui turi būti sudaryta galimybė ir sukurtos priemonės su Funkcionalumo veikimu bei naudojimu susijusiai reikiamai statistinei informacijai surinkti bei atvaizduoti administratoriaus erdvėje. Teikėjo siūlomi sprendiniai ir priemonės bei statistinės informacijos imtis turi būti suderinti su RC. Teikėjas turi atsižvelgti į RC siūlymus.

Funkciniai reikalavimai, susiję su medicininių vaizdų peržiūros įrankiu:

Reikalavimo Nr.	Aprašymas
FR_11.	Vaizdų peržiūra turi būti vykdoma interneto naršyklės pagalba.
FR_12.	Komponentas turi identifikuoti naudotojus ir autorizuoti naudotojo teises medicininio vaizdo peržiūros metu, pagal ESPBI IS veikiantį naudotojų prieigos teisių mechanizmą.
FR_13.	Komponentas turi turėti galimybę pakeisti naudotojo sąsają tarp lietuvių ir anglų kalbų.
FR_14.	Peržiūros įrankyje turi būti realizuotos šios DICOM rinkmenų peržiūros funkcijos, bet jomis neapsiribojant: 1. vaizdo didinimas, mažinimas; 2. vaizdo invertavimas; 3. vaizdo pasukimas; 4. medžiagos tankio matavimas; 5. vaizdo lango pločio / lygio parametrų keitimas; 6. vaizdo mastelio keitimas; 7. kampo matavimas; 8. pjūvių pozicijos atvaizdavimas;
FR_15.	Peržiūros įrankis turi galimybę rodyti video DICOM formato tyrimų rezultatus (formatų palaikymo tipų pvz. *MPEG-2, MPEG-4, AVC/H.264, MP4* ir kiti palaikomi DICOM standarto).
FR_16.	Peržiūros įrankis turi galimybę peržiūrėti ne DICOM formato rinkmenas, kurių (JPEG, GIF, PNG, TIFF, PDF ir kiti formatai) palaikymas apibūdintas DICOM standarto ir jo priedų aprašyme.
FR_17.	Peržiūros įrankis turi atvaizduoti DICOM rinkmenos metaduomenis.

Funkciniai reikalavimai, susiję su ne DICOM formato failų perdavimu:

Reikalavimo Nr.	Aprašymas

FR_18.	Turi būti galimybė į MedVAIS perduoti ne DICOM tyrimo formato įvairius multimedijos rinkmenų tipus, saugančius atvaizdų ir filmuotos medžiagos duomenis įskaitant ir PDF formatą (rinkmenų tipų pavyzdžiai (jais neapsiribojama): JPG, PNG, BMP, TIFF, PDF, MOV, MPEG, MPG, AVI, MP4, WMV, HEIC), juos transformuojant į DICOM tyrimo formatą tiek per integracinę sąsają, tiek per specialisto portalą.
FR_19.	Perduodant ne DICOM formato rinkmenas turi būti galimybė pateikti duomenis DICOM metaduomenų sudarymui. Sudaromos rinkmenos metaduomenis turi būti galima pateikti tiek per SPĮ integracinę sąsają (angl. Web Service), tiek per specialisto portalą ir sudarytos bendrosios validacijos taisyklės.
FR_20.	Perduodant ne DICOM formato rinkmeną, turi būti galimybė pasirinkti DICOM modalumo atributo reikšmę (angl. *modality*), kuri bus taikoma rinkmenai.
FR_21.	Po pateikimo į MedVAIS DICOM rinkmenas, suformuotas iš ne DICOM formato rinkmenų, turi būti galima perduoti į įstaigų PACS kaip ir medicininius vaizdus DICOM formatu išlaikant galimybę perduoti originalius duomenis.
FR_22.	Po pateikimo į MedVAIS, DICOM rinkmenų turinį, suformuotą iš ne DICOM formato rinkmenų, turi būti galima peržiūrėti vaizdų peržiūros įrankiu.
FR_23.	Ne DICOM formato failų įkėlimui turi būti atliekama validacija pagal iš anksto nustatytus kriterijus (pvz. nepateiktas asmens kodas), pateikiant klaidos pranešimą, jei failas neatitinka reikalavimų.
FR_24.	Ne DICOM formato failų įkėlimui turi būti taikomi apribojimai (pvz.: failo formatas, dydis) bei pateikiami klaidos pranešimai pagal detalios analizės ir projektavimo etapo metu nustatytas taisykles.

Funkciniai reikalavimai, susiję su duomenų registro ir duomenų saugyklos valdymo įrankio (toliau - Įrankyje) funkcionalumu:

Reikalavimo Nr.	Aprašymas
FR_25.	Įrankyje turi būti galimybė lanksčiai konfigūruoti atliekamus duomenų migravimo/perkėlimo darbus atsižvelgiant į aspektus: darbų eilės valdymas, pradinių duomenų atrinkimas, maišos algoritmo parinkimas (angl. *hash*, pvz. crc32, md5, sha256), planuojamo duomenų kelio struktūros šablono parinkimas atsižvelgiant į šaltinį ir kitus kriterijus (galima lanksčiai taikyti įvesties ir išvesties kelio priklausomybės parametrus). Teikėjo siūlomi sprendiniai ir priemonės turi būti suderinti su RC.
FR_26.	Turi būti galimybė duomenų migravimo įrankį pasiekti ir valdyti per MEDVAIS administratoriaus portalą.
FR_27.	Turi būti įgalintas prieigos teisių lygio valdymas MEDVAIS administratoriams ir įrankio naudotojams pritaikant projekto apimtyje naudojamą prieigos teisių mechanizmą.
FR_28.	Įrankyje turi būti atvaizduojama migravimo proceso užduočių būsenos (įskaitant užduočių kūrėja, kūrimo data ir laikas, vykdymo pradžia, prognozuojama pabaiga ir kiti aktualūs laukai) bei užduočių žurnalas.

Funkciniai reikalavimai, susiję duomenų nuasmeninimo funkcionalumu:

Reikalavimo Nr.	Aprašymas
FR_29.	Nuasmeninimo funkcionalumas turi turėti tinklinę paslaugą nuasmenintų medicininių vaizdų atidavimui kitoms informacinėms sistemoms mokslo ir statistikos tikslais.
FR_30.	Rinkmenų nuasmeninimas atliekamas užtikrinant originalios rinkmenos atsekamumą MedVAIS posistemėje, t.y. MedVAIS išlaikoma šifruota nuasmenintos ir originalios rinkmenos sąsaja, prieinama remiantis vartotojo teisių valdymo mechanizmu.
FR_31.	Turi būti sukurta galimybė administratoriaus portale lanksčiai nurodyti nuasmeninimo atributus kiekvienai nuasmeninimo užduočiai.
FR_32.	Turi būti galimybė nuasmeninimo funkcionalumą valdyti darbo eilių ir planinių darbų valdymo aspektais (angl. *work queue* ir *scheduled tasks*).
FR_33.	Turi būti sudaryta galimybė valdyti nuasmeninimo funkcionalumo prieigos teises administratoriaus portalo naudotojams.
FR_34.	Turi būti sudarytos galimybės konfigūruojamai nuasmeninti tiek metaduomenyse, tiek vaizduose įterptą (angl. *burned into pixel data*) jautrią duomenų imtį.
FR_35.	Turi būti sudaryta galimybė konfigūruoti minimalią nuasmeninamų duomenų imtį, kuri turėtų pirmenybę kitoms konfigūracijoms ir nuasmeninimo atvejais būtų pritaikoma pagal nutylėjimą.
FR_36.	Turi būti sudaryta galimybė valdyti nuasmeninamų duomenų imtį atsižvelgiant į asmenų (pacientų) valios išreiškimą.

Funkciniai reikalavimai, susiję su duomenų gyvavimo ciklo valdymo funkcionalumu:

Reikalavimo Nr.	Aprašymas
FR_37.	Atnaujintame MedVAIS sistemos administratoriaus portale turi būti galimybė taikyti medicininių vaizdų, kitų DICOM ir ne DICOM formato rinkmenų gyvavimo ciklo valdymo taisykles, nustatančias saugojimo atminties erdvių naudojimą.
FR_38.	Turi būti galimybė valdyti duomenų saugojimo kriterijus skirtingose atminties erdvėse pagal su paciento duomenimis susijusius ir kitus įvykius (pvz.: užregistruotas apsilankymas, pacientas prisijungė prie portalo meniu apie medicininius vaizdus ir kt.).
FR_39.	Turi būti galimybė atskirai pasirinkti rolių valdymo lange duomenų gyvavimo ciklo konfigūracijos keitimo ir peržiūros prieigos teises.

5. NEFUNKCINIŲ REIKALAVIMŲ APRAŠYMAS

5.1. Kriterijai nefunkcinių reikalavimų įgyvendinimui

Reikalavimo Nr.	Aprašymas
NFR_1.	Teikėjas privalo realizuoti visus specifikacijos reikalavimus.

NFR_2.	Šiame dokumente vartojami terminai „turi būti / turėti / veikti / užtikrinti / leisti / atitikti", „turi turėti galimybę", „turi būti galima" yra lygiaverčiai ir reiškia, kad Teikėjas privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą ir suteikti atitinkamas paslaugas. Funkcionalumas, kuris yra nurodytas būsimuoju laiku („bus", „leis", „apims") nurodo siekiamą įgyvendinti būseną ir reiškia, kad Teikėjas privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą.
NFR_3.	Teikėjas ar RC gali siūlyti alternatyvų atskiro specifikacijos reikalavimo įgyvendinimo būdą arba reikalavimo įgyvendinimo iškeitimą į lygiavertį funkcionalumą, kuris niekaip neigiamai neturėtų įtakos Pirkimo tikslui, uždaviniams ir galutiniams rezultatams bei neprieštarautų pirkimus reglamentuojančių teisės aktų reikalavimams. Kiekvienas siūlomas alternatyvus ar reikalavimą keičiantis funkcionalumas turi būti suderinamas su RC. Reikalavimo keitimo į lygiavertį funkcionalumą atveju, Teikėjas turės pateikti raštišką pagrindimą, apimantį pakeitimo poveikio ir kritiškumo aprašymą, pagrindžiant, kad pakeitimas neįtakoja viso Sistemos funkcionalumo. Taip pat turi būti atliktas iškeičiamo funkcionalumo vertinimas pagal laiko sąnaudas (detalizuojamos iškeičiamo funkcionalumo realizavimo laiko sąnaudos ir pateikiamos naujo funkcionalumo realizavimo laiko sąnaudos). Alternatyvių specifikacijos reikalavimų įgyvendinimui turi būti taikoma Paslaugų teikimo reglamente apibrėžta pokyčių valdymo procedūra.
NFR_4.	Teikėjas gali siūlyti alternatyvius architektūros realizavimo būdus, kurie užtikrintų lygiavertę ar geresnę Sistemos greitaveiką, aukštą prieinamumą, plečiamumą, interoperabilumą, palaikymą, saugumą ir patogumą. Kiekvienas siūlymas turi būti įvertintas ir patvirtintas Perkančiosios organizacijos.
NFR_5.	Visi sukurti servisai, aplikacijos turi būti patalpintos į konteinerizuotas aplinkas ir perduotos Perkančiajai organizacijai CI/CD diegimo procesams Docker formatu.

5.2. Reikalavimai Sistemos architektūrai

Reikalavimo Nr.	Aprašymas
NFR_6.	Sistemos realizacija turi remtis daugiasluoksne architektūra, kuri leistų Sistemą plėsti ir pritaikyti prie besikeičiančių poreikių. Sistema turi būti ne mažiau kaip 4-ių sluoksnių architektūros pagrindu ir turėti galimybę būti integruojama atskirų sluoksnių lygmenyse: 1. Atvaizdavimo lygmuo arba naudotojo sąsaja (angl. Presentation Layer) – turi užtikrinti naudotojo sąveiką su informacine sistema bei informacijos pateikimą naudotojui. 2. Veiklos logikos lygmuo (angl. Application Layer) – turi užtikrinti veiklos procesų ir taisyklių taikymą informacinės sistemos veikimo logikoje; 3. Integracijų lygmuo (angl. Integration Layer) turi užtikrint reikalingų duomenų mainus tiek tarp vidinių Sistemos komponentų, kur tai bus aktualu, tiek ir su išorinėmis informacinėmis sistemomis. 4. Duomenų bazės lygmuo (angl. Database Layer) – turi užtikrinti informacinės sistemos veikimui reikalingų duomenų kaupimą, tvarkymą ir pateikimą;

NFR_7.	Sistema turi būti realizuota remiantis SOA (angl. *Service–Oriented Architecture*) principais, išlaikant kuo didesnę ją sudarančių komponentų tarpusavio nepriklausomybę.
NFR_8.	Viso projekto metu turi būti vadovaujamasi DICOM standartu įtraukiant visas reikiamas standarto palaikomus technologinius mechanizmus.
NFR_9.	Sistemoje turi būti realizuota galimybė teikti informaciją ATNA formatu (angl. Audit Trail and Node Authentication) pagal poreikį užtikrinant, kad būtų žurnalizuojami visi sistemos komponentų veiksmai ir su jais susiję atributai (įskaitant, bet neapsiribojant šiais sluoksniais: steko pėdsakų (angl. stack trace), servisų pėdsakai (angl. service trace), veiklos logikos (angl. audit trail) ir kitų veiksmų (angl. action logs) žurnalizavimas).
NFR_10.	Projektuojant sistemą ir jos komponentus reikia atsižvelgti į tai, kad būtų užtikrinamas vieningo tiesos šaltinio (angl. SSOT – Single Source of Truth) principas Duomenų lygyje.
NFR_11.	Duomenų lygis turi būti realizuotas operacinių sistemų rinkmenų sistemos, duomenų bazių ir duomenų talpyklų ar saugyklų pavidalu. Duomenų lygmenyje skirtingi duomenų rinkiniai turi būti integruojami į vieną unifikuotą duomenų mainų posistemę su veiklos logikos lygmenyje esančiais komponentais.
NFR_12.	Projekto metu realizuotos sistemos funkcijos turi turėti detalų klaidų toleravimo ir tvarkymo mechanizmą (angl. Try...Catch), apkrovų ir aukšto sistemos prieinamumo valdymą taikant horizontalų resursų plėtimo principą (angl. horizontal scaling).
NFR_13.	Sistemos architektūra turi būti pritaikyta įgalinti hibridinį duomenų modelį nepaisant to, kad šio projekto apimtyje toks modelis nebus realizuojamas.
NFR_14.	Architektūriniai komponentai turi būti stabilūs ir plačiai naudojami praktikoje. Teikėjas negali siūlyti naudoti programinių komponentų versijų, kurios yra testavimo stadijoje, pažymėti „beta" ar kitais tai pažyminčiais būdais.
NFR_15.	Architektūriniai projektavimo principai pateikti schemoje žr. 6 pav. ir teikėjo teikiamas sprendimas turi išlaikyti DICOM standarto naudojamus duomenų apsikeitimo protokolus (pvz. WADO-RS, STOW-RS, DIMSE) tikslinėms jų funkcijoms atlikti.

5.3. Reikalavimai medicininių vaizdų peržiūros įrankiui

Reikalavimo Nr.	Aprašymas
NFR_16.	Komponentas turi veikti naudojant šias naršykles: 1. Microsoft Edge, nuo 128 ver.; 2. Mozilla Firefox, nuo 128 ver.; 3. Google Chrome, nuo 128 ver.; 4. Safari , nuo 18 ver. Komponentas neturi reikalauti jokių papildomų programinių priemonių ar įskiepių interneto naršyklėje įdiegimo.
NFR_17.	Komponentas turi pilnai integruotis su ESPBI IS ir su kitais MedVAIS komponentais bei turi veikti kaip integruotas ESPBI IS e. Sveikatos portalo komponentas.

NFR_18.	Komponentas turi palaikyti saugų duomenų perdavimą (SSL).
NFR_19.	Komponentas turi būti sertifikuotas kaip atitinkantis „EU *Medical Device Directive* 93/42/EEC" direktyvą ir turėti CE ženklą.
NFR_20.	Teikėjas savo pasiūlyme turi pateikti interneto svetainės URL nuorodą, kurioje Perkančioji organizacija galėtų ištestuoti vaizdų peržiūros priemonę pagal techninės specifikacijos reikalavimus.
NFR_21.	Peržiūros įrankis turi būti realizuotas pagal serverio ir kliento principą, kuomet vaizdų apdorojimo procesai (pvz. skirtingos kokybės medicininių vaizdų paruošimas) turi būti vykdomi serverinėje dalyje ir į kliento dalį išvedama paruošta vizualizacija (angl. *rendered*) išnaudojant WADO-RS protokolo galimybes. Dėl greitaveikos užtikrinimo tam tikros operacijos kaip vaizdo didinimas ar mažinimas (mastelio keitimas, angl. zoom) gali būti vykdomos kliento pusėje, tokių parametrų sąrašas suderinamas detalios analizė etape.
NFR_22.	Vaizdų peržiūros įrankio API privalo turėti galimybę pakeisti vaizdų peržiūros programinę įrangą (servisą) nekeičiant MedVAIS ir jos kitų komponentų architektūros, bet pakeičiant konfigūracijos parametrus (pvz. Administratoriaus erdvėje nurodant kito serviso URL ar IP adresą).
NFR_23.	Vaizdų peržiūros įrankis turi palaikyti ne mažiau nei visus DICOM standarte ir jo prieduose aprašytus palaikomų failų formatus.

5.4. Reikalavimai, susiję su duomenų registro ir duomenų saugyklos valdymo įrankiu

Reikalavimo Nr.	Aprašymas
NFR_24.	Projektuojant Įrankio veikimą turi būti atsižvelgiama, kad Įrankis turi gebėti taip valdyti išsaugotų medicininių vaizdų registrą ir medicininius vaizdus registro DB ir failų saugyklos lygiuose, kad būtų užtikrinamas perkeliamų duomenų pasiekiamumas naudotojams pagal nefunkcinių reikalavimų 5.6 dalį.
NFR_25.	Projektuojant Įrankio veikimą turi būti atsižvelgiama į Įrankio suderinimą su VNA protokolu.
NFR_26.	Įrankis turi būti projektuojamas ir suderinamas su hibridinio duomenų saugyklų modelio įgalinimu ir valdymu.

5.5. Reikalavimai technologijoms

Reikalavimo Nr.	Aprašymas
NFR_27.	Projekto realizavimui turi būti remiamasi bendrai priimtais technologiniais ir veikimo standartais (pvz. SOA, OSGi, SSL ir pan.)
NFR_28.	Esant kelioms galimoms standarto ar reikalavimo interpretacijoms, reikia laikytis geriausios praktikos principo.
NFR_29.	Visi kuriami funkciniai komponentai privalo palaikyti Unicode (UTF – 8) standartą.
NFR_30.	Projekto realizavimui turi būti atsižvelgta į naudojamų technologijų versijų palaikymo planą (angl.road-map), gyvavimo laikotarpį (angl. End of Life date) ir nenaudoti technologijų versijų paskelbtų pasenusiomis (angl. deprecated).

	Paskelbtų versijų gyvavimo pabaigos data turi būti ne trumpesnė nei 36 mėn po projekto įgyvendinimo. Išimtys turi būti suderintos su Perkančiąja organizacija.
NFR_31.	Naujos naudotojo sąsajos turi būti naudojamos Angular, React Native ar lygiavertės programinės įrangos technologijos, o modernizuojamiems naudotojo sąsajos funkcionalumams taikyti jau naudojamas technologijas kaip JavaScript, TypeScript ir kitas.
NFR_32.	Programinei įrangai kurti turi būti naudojamos JAVA ar lygiavertė technologija.
NFR_33.	Naujai kuriamų duomenų bazių technologija turi taikyti Postgres ar lygiavertę technologiją, esamų duomenų bazių ir atvejais kuomet yra būtina taikyti Oracle technologiją.
NFR_34.	Projekto realizavimui papildomai turi būti naudojamos technologijos kaip RabbitMQ, Nginx ar joms lygiavertės.

5.6. Reikalavimai Sistemos prieinamumui

Reikalavimo Nr.	Aprašymas
NFR_35.	Sistemos vidinė architektūra turi būti pritaikyta palaikyti Sistemos prieinamumą visus metus, 24 valandos per parą ir 7 dienos per savaitę - ne mažiau kaip 99,7 proc. Sistemos infrastruktūros neveikimas ir planiniai darbai, kurių metu Sistema nedirba, nėra traukiami į prieinamumo procentą.
NFR_36.	Architektūrinis sprendimas turi užtikrinti Sistemos aukštą prieinamumą (angl. High Availability, HA), kuris turi būti realizuojamas paslaugų lygyje, integracijų lygyje ir duomenų lygyje.
NFR_37.	Teikėjo siūloma Sistemos architektūra ir / ar infrastruktūra turi užtikrinti pakeičiamumo principą, t. y. įvykus vieno ar kelių komponentų gedimams, Sistema turi tęsti darbą su esamais ištekliais.
NFR_38.	Turi būti galima dirbti su Sistema, kol vykdomi kiti darbai, pavyzdžiui, atliekamų paketinių užduočių veiksmai, registravimai, naudotojo veiksmai neturi blokuoti kito naudotojo veiksmų ir neturi daryti įtakos Sistemos greitaveikai ir pan.
NFR_39.	Aukšto prieinamumo sprendimai turi veikti automatiškai (incidentų atveju). Žmogaus įsitraukimas gali būti reikalingas tik Sistemos veikimą atstatant į būseną, kuri buvo prieš incidentą.
NFR_40.	Aukšto prieinamumo sprendimas turi būti aprašytas detalios analizės ir projektavimo dokumente ir patvirtintas Perkančiosios organizacijos.

5.7. Reikalavimai plečiamumui

Reikalavimo Nr.	Aprašymas
NFR_41.	Kuriama MEDVAIS ir jos komponentai turi būti Perkančiosios organizacijos nuosavybė, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus. Pasibaigus projektui turi būti suteikta galimybė Perkančiajai organizacijai savarankiškai plėtoti ir pritaikyti MEDVAIS ir jos komponentų funkcionalumą pagal naujus kylančius poreikius, be papildomų licencijų, mokesčių ar trečiųjų šalių įsikišimo.

NFR_42.	Architektūra turi palaikyti Sistemos pajėgumų plėtros galimybes prijungiant papildomą techninę įrangą arba virtualią infrastruktūrą.
NFR_43.	Architektūra turi būti projektuojama daugiapakopės architektūros pagrindu, sudarant jos plėtros atskirų sluoksnių lygmenyse galimybes.
NFR_44.	MEDVAIS našumas turi būti nesunkiai plečiamas pridedant papildomus techninius išteklius bei techninę įrangą, nekeičiant programinės įrangos išeities tekstų. Techninės įrangos pajėgumų didinimas turi būti atliekamas nestabdant, kiek tai įmanoma, ESPBI IS darbo.
NFR_45.	MEDVAIS turi būti priemonės, užtikrinančios, kad atliekant Sistemos ir / ar atskirų jos komponentų pakeitimą ir / ar atnaujinimą, būtų išlaikomi duomenų bazės lygmenyje atlikti pakeitimai ir konfigūracijos.
NFR_46.	Programinės įrangos modifikavimas, tobulinimas ir klaidų taisymas negali turėti įtakos anksčiau įvestų duomenų vientisumui.
NFR_47.	Sistema turi būti realizuota taip, kad pereinant prie aukštesnės Sistemos versijos (keičiant / papildant Sistemos funkcionalumą) ir / arba keičiant duomenų bazę nereikėtų atlikti papildomų darbų (išskyrus tuos, kuriuos standartiškai rekomenduoja Sistemos gamintojas pereinant iš vienos Sistemos versijos į kitą).
NFR_48.	Sistemoje atliekant pakeitimą ir / ar atnaujinimą, turi būti funkcionalumas, kuris užtikrintų, kad: 1. Visi saugomi duomenys bus perkelti į naują duomenų bazės struktūrą; 2. Bus išlaikytas duomenų vientisumas ir integralumas; 3. Jokie saugomi duomenys nebus prarasti; 4. Nebus sutrikdytas Sistemoje realizuotas funkcionalumas.

5.8. Reikalavimai rezervinių kopijų darymui ir atstatymui

Reikalavimo Nr.	Aprašymas
NFR_49.	Projektas turi būti realizuotas taip, kad atliekant atnaujinimus, susijusius su architektūriniais komponentais ir / ar keičiant duomenų bazę, būtų galima atlikti visų duomenų migravimą be papildomų paslaugų ir licencijų nuomos.
NFR_50.	Rengiant rezervinę kopiją arba archyvą, neturi būti prarastos Sistemoje vykdomos transakcijos ir apdorojami duomenys, t.y., prieš rezervinės kopijos arba archyvo parengimą, turi būti užbaigiamos visos vykdomos transakcijos ir išsaugojami įvesti duomenys.
NFR_51.	Duomenų rezervinio kopijavimo procedūrų metu turi būti tenkinami greitaveikai keliami reikalavimai.

5.9. Reikalavimai sistemos monitoringui

Reikalavimo Nr.	Aprašymas
NFR_52.	Teikėjas turi sudaryti reikiamas sąlygas ir atlikti reikiamus darbus (tokius kaip paruošti ir aprašyti monitoringui reikalingus integracinius stebėsenos ir kontrolės taškus ir kt.) kad Perkančiosios organizacijos specialistai galėtų pageidaujamus komponentus prijungti prie naudojamos stebėjimo programinės įrangos (pvz.

	Zabbix, OpenTelemetry). Visi stebėsenos taškai turi būti susieti su Perkančiosios organizacijos naudojamais įrankiais.
NFR_53.	Turi būti užtikrinta galimybė WEB priemonėmis stebėti sistemos bei atskirų jos komponentų veikimo rodiklius (aktyvūs vartotojai, atminties panaudojimas, procesorių apkrova ir kiti svarbūs rodikliai) bei gauti pranešimus sutrikus komponentų veikimui ar rodikliams pasiekus kritines reikšmes. Turi būti užtikrintas Perkančiosios organizacijos specialistų informavimas, kad būtų galima sureaguoti laiku į galimus sutrikimus prieš jiems atsirandant.
NFR_54.	Visi projekto metu kuriami ar keičiami servisai turi palaikyti centralizuotą paskirstyto sekimo (ang. Service tracing) mechanizmą, užtikrinantį užklausų ir operacijų stebėjimą per visą jų vykdymo grandinę. Sekimo duomenys turi būti sugeneruoti ir perduoti naudojant Trace ID ir Span ID, kurie būtų suderinami su pasirinktu stebėjimo įrankiu (pvz. OpenTelemetry, Jaeger ar kt.).
NFR_55.	Turi būti realizuoti MEDVAIS ir jos komponentų veikimo stebėjimo ir išankstinio perspėjimo (angl. monitoring) sprendimai. Turi būti sukurta galimybė vykdyti stebėseną MEDVAIS ir jos komponentų veiklos, tinklo, serverio našumo ir kitus aktualius rodiklius pvz.: 1. vienu metu prisijungusių naudotojų kiekį; 2. CPU ir atminties apkrovą; 3. tinklo pralaidumas; 4. vidutinę sesijos trukmę; 5. laiką, per kurį sistema pateikia vaizdą klientui (taikoma peržiūros įrankiui); Pateikti rodikliai yra tik pavyzdiniai, tai nėra galutinis sąrašas. Teikėjas turės išskirti, kritinės svarbos ir kitus parametrus (iki 10 rodiklių kiekvienam iš komponentų tipų (vaizdų peržiūros įrankis, migravimo įrankis ir kt.). Visi stebėsenos taškai, kuriuose tikrinami šie ir kiti parametrai turės būti pasiūlyti Teikėjo, suderinti su Perkančiąja organizacija bei aprašyti detalios analizės ir projektavimo etapo metu.

5.10. Reikalavimai duomenų modeliui

Reikalavimo Nr.	Aprašymas
NFR_56.	Teikėjas vykdydamas projektą duomenų valdymui turi taikyti vieno karto (ang. Once only) principą siekiant kuo mažiau duomenų saugoti, o remtis užklausomis į pirminius šaltinius.
NFR_57.	Turi būti naudojamos iš anksto agreguotų duomenų lentelės (ang. pre – aggregated) agregavimui ir paieškos lentelės (ang. lookup tables) papildomai informacijai išgauti, kad sumažinti pagrindinių duomenų apdorojimo apkrovą ir užtikrintų užklausų optimizavimą.
NFR_58.	Projektuojant šio projekto realizaciją, turi būti nuolatos pildomas ir su Perkančiąją organizacija derinamas struktūrizuotų duomenų sąrašas.
NFR_59.	Visi techninėje specifikacijoje įvardinti šio projekto veiklos duomenys turi būti realizuoti projekto duomenų modelyje. Teikėjas turi realizuoti visas duomenų

	esybes (kartu su atributais ir sąsajomis), kurios yra būtinos siekiant sukurti specifikacijoje įvardintas funkcijas.
NFR_60.	Projektuojant šio projekto duomenų modelį medicininių vaizdų registras turi būti suderinamas su hibridinio modelio architektūros principais.
NFR_61.	Teikėjas privalo migruoti esamo duomenų registro įrašus (Oracle DB duomenis) ir medicininių vaizdų saugyklos (StorNext diskinių saugyklų) duomenis į modernizuotą sistemą pagal suderintą migracijos darbų planą.

5.11. Reikalavimai Sistemos administravimui

Reikalavimo Nr.	Aprašymas
NFR_62.	Sistemos administratorius turi turėti galimybę sukurti Sistemos administratorių prisijungimo duomenis (prisijungimo vardą ir slaptažodį), įvesti vardą ir pavardę, el. pašto adresą ar panaudoti jau esamus prisijungimo mechanizmus.
NFR_63.	Sistemos administratorius turi turėti galimybę valdyti naudotojų prieigos teises.
NFR_64.	Sistema neturi riboti registruotų Sistemos naudotojų skaičiaus.
NFR_65.	Sistemos administratorius turi galėti peržiūrėti Sistemos naudotojų veiksmų audito žurnalą, kuriame bus fiksuojami visi naudotojų veiksmai, jų gaunami sisteminiai klaidų pranešimai, taip pat kokie duomenys į kokius buvo pakeisti. Turi būti fiksuojama veiksmo data, laikas, naudotojo vardas, interneto prieigos naudotojų tinklo IP adresas arba vidinio tinklo naudotojų IP ir MAC adresai.
NFR_66.	Turi būti sudaryta galimybė naudotojams matyti jų prieigos teisių lygį. Šis matomumas turi būti valdomas Sistemos administratoriaus.

5.12. Reikalavimai našumui ir greitaveikai

Reikalavimo Nr.	Aprašymas
NFR_67.	Naujos projekto funkcijos turi atitikti greitaveikos reikalavimus: 1. Detalaus lango (su visais norimais objektais) atidarymas turi trukti ne ilgiau nei 2 sekundes; 2. Duomenų išsaugojimo operacija po keitimo turi trukti ne ilgiau nei 1 sekundę; 3. Duomenų mainuose dalyvaujančių žiniatinklio paslaugų atsakymai turi būti pateikiami per ne ilgiau nei 2 sekundes; 4. Meniu sąrašo (Sistemos funkcijų pasirinkimo) naudotojams pateikimas turi trukti ne ilgiau nei 1 sekundę; 5. Navigacija tarp skirtingų Sistemos naudotojo sąsajos langų (tiek naujo lango atidarymas, tiek lango pakeitimas) turi trukti ne ilgiau kaip 2 sekundes (išskyrus atvejus, kai generuojama ataskaita); 6. Navigacija tarp skirtingų duomenų įvedimo laukų turi trukti ne ilgiau kaip 2 sekundes (išskyrus atvejus, kai generuojama ataskaita); 7. Sąrašo reikšmių pateikimas (konkretaus klasifikatoriaus reikšmių) turi trukti ne ilgiau nei 1 sekundę;

	8. Duomenų paieška sistemoje, baigtinio paieškos rezultato atvaizdavimas iki 5 (penkių) sekundžių, išskyrus kompleksinėms, sudėtingoms užklausoms; 9. Automatinės (paketinės, foninės) užduotys (masiniam duomenų apdorojimui) – Sistema turi apdoroti ne mažiau 100 objektų per 1 sekundę (visi tarpiniai duomenų apdorojimai, veiksmai su duomenimis, duomenų rašymai į tarpines lenteles ir pan. turi būti atliekami per tą patį laiką). Projekto metu su Perkančiąja organizacija gali būti suderintos funkcijos, kurioms nėra taikomos šiame reikalavime numatytos trukmės ir gali būti suderinti konkretūs sudėtingi atvejai (pavyzdžiui, kurių metu atliekamas informacijos agregavimas), kuriems taikomos kitos greitaveikos trukmės. Šie išimtiniai atvejai gali būti taikomi tik gavus Perkančiosios organizacijos patvirtinimą. Greitaveikos reikalavimai neapima Užsakovo infrastruktūros interneto ryšio.
NFR_68.	Teikėjas turi pateikti Perkančiajai organizacijai greitaveikos testavimo aplinką.
NFR_69.	Teikėjas turės atlikti sistemos apkrovų toleravimo testavimą ir pateikti ataskaitą Perkančiajai organizacijai. Vaizdų peržiūros įrankis turi būti išbandytas iki 2 kartų didesne nei numatyta apkrova, ir neprarasti veikimo stabilumo, o galima tik suprastėjusi greitaveika. Teikėjas įsipareigoja išspręsti visus testavimo metu rastus trūkumus, jeigu testų rezultatai netenkins visų įvardintų našumo ir greitaveikos reikalavimų. Apkrovos testavimo scenarijai: 1. Vartotojo prisijungimo testai. Simuliuoti daug vartotojų tuo pačiu metu prisijungiant prie platformos. 2. Vaizdų peržiūrų testai. Simuliuoti daug vartotojų, kurie tuo pačiu metu peržiūri skirtingus medicininius vaizdus. 3. Apkrovos testai. Testuoti, kaip sistema veikia su dideliu vartotojų kiekiu – nuo kelių iki keliasdešimt tūkstančių. 4. Patikimumo ir stabilumo testai. Simuliuoti ilgalaikes vaizdų peržiūros sesijas su pilnos darbo dienos valandų trukme. 5. Galimų išteklių ribų nustatymas pagal apkrovos lygiu intervalus. Simuliuoti scenarijus, kai išteklių ribos pasiekiamos (CPU, RAM, tinklo pralaidumo ir kt.).
NFR_70.	Turi būti realizuotas funkcijų ir atliekamų naudotojų veiksmų, kurios viršija nustatytus našumo reikalavimus aprašytus aukščiau, auditavimas. Audito įraše turi būti pakankamai duomenų, kad būtų galima nustatyti, kuris projekto komponentas ar/ir funkcija netenkina arba padidina riziką tam tikromis aplinkybėmis netenkinti našumo reikalavimų.
NFR_71.	Projekto apimtyje turi būti indikuojami ilgiau trunkantys procesai (atliekamos funkcijos) ir naudotojo sąsajoje turi būti aiškiai įvardinta, kuomet ESPBI IS, MedVAIS ir jų komponentai veikia tinkamai (pvz. didelės apimties medicininio vaizdo atsiuntimas)
NFR_72.	Automatinių (foninės, paketinės, ataskaitų) užduočių vykdymas neturi daryti įtakos Sistemos naudotojų darbui.
NFR_73.	Integracinių sąsajų realizacija turi užtikrinti, kad projektavimo metu apibrėžti integraciniai scenarijai įvyks per racionalų laiko intervalą ir niekaip nedarys neigiamos įtakos ESPBI IS naudojimo patogumui ir našumui.

5.13. Reikalavimai programinei įrangai ir programinės įrangos licencijoms

Reikalavimo Nr.	Aprašymas
NFR_74.	Sistemos programinė įranga turi būti instaliuojama tarnybinėje stotyje. Naudotojo kompiuteryje (darbo vietoje) neturi būti instaliuojami jokie Sistemos komponentai.
NFR_75.	Visa sprendimo programinė įranga, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus, kuri bus sukurta Projekto vykdymo apimtyje turi būti pilnai perduota Perkančiajai organizacijai (perduodamos visos turtinės teisės ir išeities kodai bei konfigūracijos).
NFR_76.	Sistema turi būti kuriama taip, kad duomenys ir verslo logika būtų laikomi konfigūruojamose saugyklose arba išoriniuose šaltiniuose, o ne įterpti tiesiogiai į programinį kodą (angl. not Hard Coded).
NFR_77.	Projekto metu sukurtos programinės įrangos išeities tekstai Perkančiajai organizacijai turi būti perduoti Docker formatu paruoštų rinkmenų paketų forma nurodant standartines kompiliavimo priemones ir kompiliavimo eigą bei su kompiliavimo scenarijų išeities tekstais, o kuriamas kodas turi būti saugomas RC Git repozitorijoje.
NFR_78.	Projekto metu sukurtos / modernizuotos programinės įrangos išeities tekstai turi būti su išsamiais komentarais ir atitikti gerąsias programinio kodo formatavimo, kintamųjų bei funkcijų įvardinimo praktikas įskaitant, tačiau neapsiribojant praktika, kai pagal pavadinimą galima suprasti programinio kodo elemento paskirtį ir praktiką, kai kodo formatavimas leidžia suprasti kodo struktūrą.
NFR_79.	Programinio kodo išeities tekstams turi būti taikomas ISO/IEC 5055:2021 ar lygiavertis(-čiai) standartas(-ai), kurio faktinio taikymo apimtis atsižvelgiama pagal naudojamas technologijas ir suderinama su Perkančiąja organizacija. Teikėjas išeities tekstų kokybei valdyti turi paruošti modulių (angl. Unit test) testus ir kitus darbo vykdymo reglamente numatytas dalis, kurios įgalina CI/CD procesą naudojant gerąsias praktikas ir automatinius testavimus (pvz. pasitelkiant įrankius, bet neapsiribojant, kaip SonarQube ar lygiaverčius).
NFR_80.	Pagrindiniam tvarkytojui turi būti perduoti pilni, korektiški išeities tekstai, iš kurių naudojant standartines ir viešai prieinamas priemones, būtų kompiliuojama parengta naudojimui programinė įranga, atliekanti jai specifikuotas funkcijas.
NFR_81.	Posistemės modernizavimui naudojant papildomą licencinę programinę įrangą, tokios įrangos licencijavimo tvarka turi būti nuolatinio galiojimo (be jokių galiojimo apribojimų laike ir be jokių papildomų mokesčių norint plėsti ar palaikyti funkcionalumus) kad Perkančiajai organizacijai nereikėtų įsigyti papildomų licencijų ar kitaip patirti išlaidų programinės įrangos veikimui. Teikėjas turi pateikti tokią programinę įrangą ir licencijas visoms numatomoms įdiegti IS aplinkoms (testavimo, mokymų bei produkciniai aplinkai).
NFR_82.	Kiekviena siūloma panaudoti papildoma licencijuojama PĮ turi būti suderinama su Perkančiąja organizacija.
NFR_83.	Siūlant papildomą licencinę programinę įrangą, jos įsigijimo ir ne mažiau kaip 3 metų (skaičiuojant nuo testavimo etapo pabaigos) gamintojo užtikrinto palaikymo kaina turi būti įskaičiuota į pasiūlymo kainą.

NFR_84.	Teikėjas turi garantuoti nuostolių atlyginimą Perkančiajai organizacijai dėl bet kokių reikalavimų, kylančių dėl autorių teisių, patentų, licencijų ar prekių (paslaugų) ženklų naudojimo, susijusio su sukurtos programinės įrangos naudojimu, išskyrus atvejus, kai toks pažeidimas atsiranda dėl Perkančiosios organizacijos kaltės.
NFR_85.	Programinė įranga su kompiliavimo išeities tekstais turi būti perduodama Docker konteinerių formatu, užtikrinant visų priklausomybių ir vykdymui reikalingų komponentų įtraukimą.
NFR_86.	Perduodami išeities tekstai (angl. source code) pateikiami tik elektroninėje formoje ir turi atitikti šiuos reikalavimus: 1. Išeities kodas prieš kiekvieną diegimą turi būti padėtas į Perkančiosios organizacijos GIT aplinką ir iš ten paruošti diegimo paketai į testinę bei gamybinę aplinkas. 2. Išeities tekstai Perkančiajai organizacijai turi būti perduoti kompiliavimui paruoštų rinkmenų paketų forma, nurodant standartines kompiliavimo priemones, kompiliavimo eigą ir kartu su visomis kompiliavimui reikalingomis bibliotekomis; 3. Išeities tekstai turi būti su išsamiais komentarais ir atitikti gerąsias programinio kodo formatavimo, kintamųjų bei funkcijų įvardinimo praktikas įskaitant, tačiau neapsiribojant praktika, kai pagal pavadinimą galima suprasti programinio kodo elemento paskirtį ir praktiką, kai kodo formatavimas leidžia suprasti kodo struktūrą. 4. Išeities kodas turi 70 – 80 % padengtas automatiniais testais (unit tests). Turi būti užtikrintas visų funkcijų, vartotojo sąsajų ir integracijos testavimas. 5. Perkančiajai organizacijai turi būti perduoti pilni, korektiški išeities tekstai, iš kurių naudojant standartines priemones būtų kompiliuojama naudojimui parengta programinė įranga, atliekanti jai specifikuotas funkcijas. 6. Turi būti parengtas priėmimo testavimo išeities tekstų testas atliekant išeities tekstų kompiliavimą Perkančiosios organizacijos aplinkoje ir funkcinį kompiliavimo metu gautos versijos testavimą. 7. Garantinio aptarnavimo metu Teikėjui atlikus programinės įrangos pakeitimus, išeities tekstai turės būti atnaujinti ir pateikti pagal aukščiau nurodytuose punktuose nustatytas sąlygas.
NFR_87.	Projekto kompiliavimas, konfigūravimas ir diegimas turi būti atliekamas iš programinio kodo saugyklų, esančių Perkančiosios organizacijos infrastruktūroje, naudojant automatizuotas nuolatinės integracijos (angl. Continuous integration) priemones. Atvejais kai tokių priemonių trūksta Teikėjas turi įdiegti Pagrindinio tvarkytojo infrastruktūroje.
NFR_88.	Teikėjas turi pateikti ir į pasiūlymo kainą įskaičiuoti visą reikiamą standartinę ir nestandartinę programinę įranga, jeigu to reikia, kad būtų užtikrintas funkcionalumas ir našus darbas (tenkinantis našumo reikalavimus).
NFR_89.	Esant poreikiui Teikėjas turi atlikti techninės įrangos konfigūracijas. Jos turi būti atliktos iš Perkančiosios organizacijos nereikalaujant papildomų lėšų.

NFR_90.	Naujos programinės įrangos funkcionalumo ir funkcionalumo pakeitimų realizavimas neturi pareikalauti papildomos techninės ir licencijuojamos standartinės ir nestandartinės programinės įrangos įsigijimo Perkančiajai organizacijai.

5.14. Reikalavimai integracinėmis sąsajoms

Reikalavimo Nr.	Aprašymas
NFR_91.	Sistemoje turi būti realizuotos šio dokumento reikalavimuose pateiktos preliminarios integracinės sąsajos. Detalios integracinės sąsajos turės būti suderintos Projekto metu.
NFR_92.	Sistemoje turi būti realizuoti detaliosios analizės ir projektavimo etapo metu suderinti reikalingi integraciniai taškai. Teikėjas turi aiškiai apibrėžti ir aprašyti integracinių taškų specifiką. Pavyzdinė aprašymo struktūra: 1. Integracinio taško pavadinimas; 2. Tikslas; 3. Aprašymas; 4. Duomenų šaltinis (pvz., naudotojo veiksmai, DB žurnalai, API užklausos); 5. Duomenų perdavimo mechanizmas (HTTP, REST API ir t.t); 6. Protokolas (pvz., HTTPS); 7. Duomenų formatą (pvz. JSON, XML); 8. Teikiamų duomenų turinio išsamūs pavyzdžiai.
NFR_93.	Sistemos integracinės sąsajos turi būti realizuotos naudojant aplikacijų programavimo sąsaja (angl. Application Programming Interface, API).
NFR_94.	Teikėjas turi parengti ir suderinti integracinės sąsajos techninę specifikaciją, t.y., parengti projektinę integracinės sąsajos dokumentaciją, kurios pagrindu kita šalis turės atlikti reikalingus informacinės sistemos vystymo darbus, susijusius su reikiama integracine sąsaja.
NFR_95.	Posistemei aktualūs vidiniai ir išoriniai duomenų mainai turi būti vykdomi naudojant esamas ESPBI IS priemones.
NFR_96.	Teikėjas turi užtikrinti, kad nebus sutrikdytas jau veikiančių integracinių sąsajų veikimas.
NFR_97.	Sąsajos turi teikti aiškias klaidų žinutes (pvz., HTTP atsakymus su kodais: „400 Bad Request", „503 Service Unavailable").
NFR_98.	Sąsajos turi palaikyti didelį naudotojų kiekį vienu metu. Turės būti atlikta apkrovos analizė (angl. Stress analysis) ir jos rezultatai pateikti Perkančiajai organizacijai.

5.15. Reikalavimai naudotojų sąsajai ir patogumui naudoti

Reikalavimo Nr.	Aprašymas
NFR_99.	Naudotojo sąsaja turi atitikti pirkimo metu vyraujančias dizaino tendencijas ir suderinta su Perkančiosios organizacijos identitetu (spalvos, šriftai). Naudojo sąsajos pavyzdžiai gali būti pateikiami atskiromis dalimis: naudotojo sąsajos ir

	patogumui naudoti (angl. UI and UX). Galutinis sprendimas iš pateiktų pavyzdžių patvirtinamas Perkančiosios organizacijos.
NFR_100.	Naudotojų sąsajos klaidų pranešimai turi būti suformuluoti taip, kad naudotojui būtų aišku, kas atsitiko ir kokius veiksmus jam toliau reikia atlikti, kad galėtų tęsti darbą.
NFR_101.	Visi to paties tipo (klaidų, įspėjamieji ir kt.) pranešimai turi būti pateikiami vienodu stiliumi (toje pačioje ekrano vietoje, tuo pačiu stiliumi, išskirti tomis pačiomis spalvomis).
NFR_102.	Naudotojo sąsaja turi būti pritaikyta pagal naudotojų ir paslaugų gavėjų tipą ir prieigos teises. Naudotojams turi būti pateikiamos tik jiems aktualios funkcijos, o darbui nereikalingi arba neleistini Sistemos funkcionalumai neturi būti matomi.
NFR_103.	Naudotojo sąsaja turi būti realizuota lietuvių ir anglų kalbomis (pasirenkant lietuvių kalbą kaip numatytąją pagal nutylėjimą) ir naudojama laikantis bendrinių kalbos taisyklių. Teikėjas detalios analizės ir projektavimo etapo metu turi suderinti vertimus su Perkančiąją organizacija.
NFR_104.	Turi būti vykdomas loginis duomenų laukų tikrinimas laukų lygiu (pvz.: asmens varde negali būti skaičių) ir laukų grupių lygiu (pvz.: paieškos pradžios data turi būti ankstesnė nei paieškos pabaigos data). Prieš išsaugant pateiktus duomenis turi būti atliekamas išsamus loginis jų patikrinimas (pvz.: ar visi privalomi laukai užpildyti).
NFR_105.	Duomenų įvedimo formose duomenų laukai turi būti užpildomi automatiškai, jeigu Sistemos duomenų bazėje ar integruotose duomenų bazėse yra saugomi atitinkami duomenys.
NFR_106.	Naudotojo sąsajoje visada turi būti matomas pilnas ir interaktyvus navigacijos kelias (angl. Breadcrumbs).
NFR_107.	Naudotojo sąsaja turi prisitaikyti prie įvairaus dydžio ekranų (ang. Responsive design).
NFR_108.	Prie sudėtingų funkcijų ar informacijos blokų turi būti galimybė pateikti kontekstinę pagalbą.
NFR_109.	Visi kuriami ar keičiami funkciniai komponentai turi korektiškai saugoti, apdoroti ir atvaizduoti informaciją lietuvių ir anglų kalbomis su specifiniais lietuvių kalbos rašmenimis ir taisyklėmis.

5.16. Reikalavimai duomenų archyvavimui

Reikalavimo Nr.	Aprašymas
NFR_110.	Turi būti galimybė nustatyti duomenis ar duomenų grupes, kurie gali būti archyvuojami ir realizuotas automatinis mechanizmas, kuris užtikrintų šių duomenų archyvavimą. Duomenų archyvavimo sprendimas turi būti suderintas su Perkančiąja organizacija.
NFR_111.	Duomenys turi būti perkeliami į duomenų archyvą pagal projekto analizės etape suderintus kriterijus.

5.17. Reikalavimai standartų taikymui

Reikalavimo Nr.	Aprašymas
NFR_112.	MEDVAIS posistemė turi būti įgyvendinta vadovaujantis ISO 12052:2017 standarto DICOM palaikymas yra privalomai taikomas.
NFR_113.	MEDVAIS posistemė turi būti įgyvendinta vadovaujantis ISO 10781:2023 „Elektroninės sveikatos istorijos informacinės sistemos funkcinis modelis, antrasis papildytas leidimas“ (angl. Electronic Health Record-System Functional Model, Release 2.1) ar naujesniu lygiaverčiu standartu.
NFR_114.	ISO/IEC 5055:2021 ar lygiavertis(-čiai) standartas(-ai), kurio tikslai yra apibrėžti kuriamos programinės įrangos išeities kodo kokybę ir automatizuotą išeities kodo kokybės tikrinimą. Pasirinkto standarto taikymo apimtis aptariama atsižvelgiant į naudojamas technologijas ir suderinama su Perkančiąja organizacija detalios analizės etape.
NFR_115.	Naudotojo sąsaja turi atitikti WCAG 2.2 lygio prieinamumo reikalavimus.
NFR_116.	Naudotojo sąsaja turi atitikti W3C HTML5 ir CSS3 standartus.
NFR_117.	Naudotojo sąsaja turi būti kuriama laikantis LST EN ISO 9241 standartų šeimos ergonomikos reikalavimų ir rekomendacijų.
NFR_118.	Teikėjo rengiamuose ESPBI IS analizės ir projektavimo dokumentuose, veiklos procesų schemų, modelių, duomenų bazių schemų, programinių komponentų sąsajų schemų ir kitų esybių sąsajų schemų projektavimui turi būti naudojama ne žemesnė kaip 2.0 UML (angl. Unified Modeling Language) arba BPMN 2.0 (angl. Business Process Model and Notation) standarto versija.
NFR_119.	Turi būti naudojamas šifravimo standartas AES (angl. Advanced Encryption Standard) arba lygiavertis ar naujesnis.
NFR_120.	Sukurta programinė įranga turi atitikti tarptautinius saugumo standartus LST ISO/IEC 27002, LST ISO/IEC 27001 ar lygiaverčius standartus.
NFR_121.	Turi būti palaikomas X.509 arba naujesnis standartas naudojant skaitmeninius sertifikatus sąveikose: sistema – sistema ir sistema – naudotojas.
NFR_122.	Norint užtikrinti saugų internetu perduodamų duomenų perdavimą, turi būti naudojamas TLS (Transport Layer Security) protokolas, versija 1.2 arba naujesnė, tiek komunikacijoje tarp sistemos ir naudotojo, tiek, jei reikalinga, ir tarp sistemų.

6. REIKALAVIMAI PASLAUGŲ TEIKIMUI

6.1. Reikalavimai darbo vietai

Reikalavimo Nr.	Aprašymas
PR-1.	Pagal numatytas procedūras Paslaugų teikėjo darbuotojams dalyvaujantiems Pirkimo objekto vykdyme (toliau – Teikėjo specialistai), suteiks prieigą prie Perkančiosios organizacijos išteklių (toliau – prieiga): 1. Teikėjo specialistams bus suteikta prieiga prie Perkančiosios organizacijos aplikacijų: JIRA, CONFLUENCE;

	2. Teikėjo specialistams, aplikacijų programuotojams bus suteikta prieiga prie Perkančiosios organizacijos GIT saugyklos, skirtos Pirkimo objekto programinės įrangos pirminio kodo versijų valdymui, bei prie serverių, skirtų Pirkimo objekto vykdymui infrastruktūros plėtros aplinkoje (DEV) (nesuteikiant administracinių teisių) ir reikalingų duomenų bazių (DB) schemų. Pagal poreikį, Perkančioji organizacija suteiks saugią nuotolinę prieigą – dedikuotą virtualią darbo vietą (angl. Virtual Desktop Infrastructure, toliau – VDI), per kurią Teikėjo specialistai pasieks Perkančiosios organizacijos išteklius reikalingus Paslaugų teikimui.
PR-2.	Pagal poreikį, Perkančioji organizacija galės suteikti Teikėjo specialistų kompiuterinėms darbo vietoms saugią nuotolinę VPN prieigą prie jiems dedikuotų išteklių reikalingų Pirkimo objekto vykdymui.
PR-3.	Teikėjo specialistams nebus suteikta prieiga prie Perkančiosios organizacijos produkcinių duomenų, ar produkcinių aplinkų. Visi kūrimo, testavimo ir priežiūros darbai bus vykdomi Perkančiosios organizacijos kūrimo (DEV) ir testavimo (TEST) aplinkose, naudojant Perkančiosios organizacijos pateiktus nuasmenintus arba testinius duomenis.

6.2. Reikalavimai paslaugų užsakymui

Reikalavimo Nr.	Aprašymas
PR-4.	Paslaugų teikėjas gali teikti papildomas paslaugas, kurių apimtyje Perkančioji organizacija gali užsakyti papildomus funkcionalumus. Vystymo paslaugų apimtis – iki 300 val.
PR-5.	Papildomo funkcionalumo užsakymo tvarka: 1. identifikuojamas papildomo funkcionalumo poreikis; 2. poreikis patvirtinamas Perkančiosios organizacijos; 3. Paslaugų teikėjas parengia siūlymą, kuriame aprašo papildomo funkcionalumo realizavimo principus, realizavimo terminą ir įvertina realizacijai reikalingą valandų skaičių (žr. 8.1.1 priedas. Papildomų paslaugų užsakymo forma); 4. Perkančiajai organizacijai patvirtinus siūlymą, siūlymo pagrindu formuojamas papildomas funkcionalumo užsakymas, kuris pasirašomas Perkančiosios organizacijos ir Paslaugų teikėjo.
PR-6.	Papildomais funkcionalumais negali būti laikomi šiame RPO apibrėžti reikalavimai, juos detalizuojantys sprendimai
PR-7.	Patvirtintos paslaugos bus užsakomos Perkančiosios organizacijos JIRA pateikiant užduotis – konkrečios užduotys priskiriamos Teikėjo specialistui(-ams), kuriems prieš tai suteikiama prieiga prie Perkančiosios organizacijos JIRA (žr. RPO PR-1 papunktį).
PR-8.	Mažiausiai 12-os mėnesių garantija turi būti taikoma visoms papildomai užsakytoms paslaugoms.

6.3. Reikalavimai RPO įgyvendinimui

Reikalavimo Nr.	Aprašymas
PR-9.	Paslaugų teikėjas privalo realizuoti RPO reikalavimus.
PR-10.	Paslaugų teikėjas ar Perkančioji organizacija gali siūlyti alternatyvų atskiro RPO reikalavimo įgyvendinimo būdą, arba reikalavimo įgyvendinimo iškeitimą į lygiavertį funkcionalumą, kuris niekaip neigiamai neturėtų įtakos Pirkimo tikslui, uždaviniams ir galutiniams rezultatams, bei neprieštarautų pirkimus reglamentuojančių teisės aktų reikalavimams. Kiekvienas siūlomas alternatyvus, ar reikalavimą keičiantis funkcionalumas, turi būti suderinamas su Perkančiąja organizacija. Reikalavimo keitimo į lygiavertį funkcionalumą atveju, Teikėjas turės pateikti raštišką pagrindimą, apimantį pakeitimo poveikio ir kritiškumo aprašymą, pagrindžiant, kad pakeitimas neįtakoja viso Sistemos funkcionalumo. Taip pat turi būti atliktas iškeičiamo funkcionalumo vertinimas pagal laiko sąnaudas (detalizuojamos iškeičiamo funkcionalumo realizavimo laiko sąnaudos ir pateikiamos naujo funkcionalumo realizavimo laiko sąnaudos). Alternatyvių specifikacijos reikalavimų įgyvendinimui turi būti taikoma Paslaugų teikimo reglamente apibrėžta pokyčių valdymo procedūra. Teikėjas gali siūlyti alternatyvius architektūros realizavimo būdus, kurie užtikrintų lygiavertę ar geresnę Sistemos greitaveiką, aukštą prieinamumą, plečiamumą, interoperabilumą, palaikymą, saugumą ir patogumą. Kiekvienas siūlymas turi būti įvertintas ir patvirtintas Perkančiąja organizacija.
PR-11.	Teikėjas kartu su pasiūlymu turi pateikti siūlomos programinės įrangos techninę dokumentaciją bei dokumentus, patvirtinančius, kad Teikėjas yra siūlomos įrangos gamintojas arba oficialus gamintojo atstovas ir (ar) įgaliotas partneris, turintis teisę parduoti bei diegti ir (ar) konfigūruoti siūlomą įrangą.
PR-12.	Teikėjas kartu su Sutartimi, pasirašo asmens duomenų tvarkymo susitarimą.
PR-13.	Teikėjas užtikrina, kad asmuo, vykdysiantis Sutarties Techninės dalies įgyvendinimą pasirašytų Perkančiosios organizacijos pateiktą Konfidencialumo pasižadėjimą.
PR-14.	Teikėjas privalo vadovautis Sutarties vykdymo metu aktualiomis teisės aktų redakcijomis. Teikėjui privalomi ir visi Sutarties vykdymo metu naujai priimti / pakeisti teisės aktai, jeigu jie susiję su Sutarties įgyvendinimu. Jei naujai priimti / pakeisti teisės aktai prieštarauja Techninėje specifikacijoje aprašytiems reikalavimams, Teikėjas turi įgyvendinti reikalavimus vadovaudamasis Sutarties vykdymo metu priimtų / pakeistų teisės aktų versijomis.
PR-15.	Per 5 darbo dienas nuo Sutarties įsigaliojimo Paslaugų teikėjas turi surengti įvadinį susitikimą su Registrų Centru bei pateikti derinimui ir pristatyti Paslaugų teikimo reglamentą (pagrindinės dalys nurodytos 4-oje lentelėje)
PR-16.	Teikėjas turės bendrauti su Perkančiąja organizacija susitikimų metu, raštu ir e. paštu, ir dalyvauti rengiamų dokumentų aptarime su suinteresuotomis šalimis bei suteikti pagalbą pristatant ir aptariant pateikiamų dokumentų turinį bei teikti kitas su Specifikacijos parengimu susijusias konsultacijas Registrų centrui. Visų susitikimų turinys turi būti protokoluojamas taip kaip nurodyta Paslaugų teikimo reglamente.

PR-17.	Paslaugų teikėjas yra atsakingas už reikalingų įrankių ir techninės įrangos įsigijimą Paslaugoms atlikti.
PR-18.	Teikėjo pasiūlyti specialistai turi gebėti žodžiu ir raštu bendrauti lietuvių ir anglų kalbomis (ne mažesniu nei C1 lygiu pagal Bendrąją Europos kalbų mokėjimo orientacinę sistemą). Jei specialistas nemoka lietuvių ar anglų kalbos, reikalavimas gali būti įvykdytas užtikrinant vertimo paslaugas Sutarties vykdymo metu, kurios turi būti įtrauktos į pasiūlymo kainą.

6.4. Reikalavimai paslaugų teikimo etapams ir programinės įrangos kūrimo iteracijoms

4 lentelė. Paslaugų įgyvendinimo etapai

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Inicijavimas	Teikėjas: 1. Parengia Paslaugų teikimo reglamentą, detalų darbų grafiką ir suderina su Perkančiąja organizacija. Perkančioji organizacija: 1. Suteikia reikalingą informaciją; 2. Teikia pastabas ir rekomendacijas.	1. Parengtas Paslaugų teikimo reglamentas. Paslaugų teikimo reglamente nurodoma projekto tikslai, prioritetai, etapų apimtys ir rezultatai, suinteresuotos šalys, darbų atlikimo grafikas, kokybiniai reikalavimai, rizikos ir jų suvaldymo būdai, komunikavimo principai, atsakomybės, tarpinių ir galutinių rezultatų priėmimo kriterijai, papildomų užsakymų valdymo procedūra ir kita svarbi informacija. 2. Parengtas detalus darbų grafikas ir pateikti pagrindiniai riboženkliai (angl. milestones)	Etapo rezultatai turi būti pateikti ir suderinti su Perkančiąja organizacija ne vėliau kaip per 10 darbo dienų nuo Paslaugų teikimo sutarties įsigaliojimo datos.
Detali analizė	Teikėjas: 1. Atlieka esamos ir siekiamos padėties įvertinimą; 2. Parengia detalios analizės dokumentaciją; 3. Vykdo kitas veiklas numatytas analizės etapo metu. Perkančioji organizacija: 1. Suteikia reikalingą informaciją; 2. Teikia pastabas ir rekomendacijas; 3. Tvirtina pateiktus etapo rezultatus.	1. Parengtas detalios analizės dokumentas, kuriame išanalizuojami ir detalizuojami funkciniai ir nefunkciniai RPO reikalavimai bei kiti Perkančiosios organizacijos išsakyti poreikiai, parengiami naudotojų pasakojimai (angl. User Story) ir panaudojimo atvejai (angl. use case), kurie pateikiami panaudos atvejų diagramomis pagal UML (angl. Unified Modeling Language) notaciją ir detalizuojami aprašant kiekvieno panaudos atvejo vykdymo žingsnius (pagrindinę eigą, alternatyvią eigą, išimtinę eigą) ir kitus apribojimus. Jei reikia, aprašomi IS vartotojai ir jų teisės.	Pagal suderintą darbų grafiką.

Projektavimas	<u>Teikėjas:</u> 1. Atlieka projektavimą ir parengia projektavimo dokumentaciją; 2. Parengia ir suderina infrastruktūros techninį aprašymą; 3. Išanalizuoja ir parengia integracinių sąsajų aprašymo dokumentus; 4. Suderina naujas integracines sąsajas su duomenų teikėjais ir gavėjais; 5. Parengia integracinių sąsajų specifikacijas bei jas suderina su duomenų gavėjais ir teikėjais bei Perkančiąja organizacija; 6. Atnaujina ir su Perkančiąja organizacija suderina ESPBI IS techninį aprašymą. <u>Perkančioji organizacija:</u> 1. Suteikia reikalingą informaciją; 2. Teikia pastabas ir rekomendacijas. 3. Tvirtina pateiktus etapo rezultatus.	1. Sukurtas Projektavimo dokumentas (dokumente pateikiama: projekto architektūros aprašymas fizinių komponentų ir programinių komponentų požiūriu, naudojamos technologijos (jų pavadinimai, versijos), informacinis vaizdas (duomenų bazės struktūros, duomenų bazių sąsajų schemos ir kt.), funkcinis vaizdas (projekto funkciniai vienetai, jų funkcijos, tarpusavio sąsajos, naudotojo sąsajos prototipai), integracinis vaizdas (sąsajos tarp vidinių ir išorinių sistemų, kuriamos sistemos atžvilgiu), operacinis vaizdas (sisteminiai procesai, algoritmai, periodiniai sisteminiai darbai ir pan.), dislokavimo vaizdas (programinių komponentų pasiskirstymas techninėje įrangoje), saugumo sprendimai, aukšto prieinamumo sprendimai, plečiamumo sprendimai ir kt.); 2. Parengtas infrastruktūros techninis aprašymas (dokumente pateikiamas detalus techninės ir sisteminės programinės įrangos aprašymas, kuris reikalingas užtikrinant tinkamą Teikėjo siūlomo sprendimo funkcionavimą. Mažiausiai turi būti pateikiama: reikalavimai techninei įrangai; reikalavimai sisteminei programinei įrangai; papildomos techninės ir sisteminės programinės įrangos suderinamumo su esama Perkančiosios organizacijos infrastruktūra analizė ir reikalavimai.) 3. Atnaujintas/parengtas techninės architektūros dokumentas; 4. Atnaujintas/parengtas loginis DB modelis; 5. Sukurtos Integracinių sąsajų specifikacijos (sukurtos sąsajų specifikacijos ir duomenų apsikeitimo specifikacijos); 6. Atnaujintas techninis aprašymas (specifikacija); 7. Parengtos pradinės naudotojo sąsajos gairės, apimančios: 7.1. naudotojo sąsajos schemas;	Pagal suderintą darbų grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
		7.2. struktūrą ir dizainą; 7.3. parengtas pradinis naudotojų sąsajos prototipas.	

Programavimas	Teikėjas: 1. Parengia ir pateikia diegimo į testinę aplinką planą; 2. Vykdo reikalingus programavimo ir programinio konfigūravimo darbus (savo kūrimo aplinkoje), įgyvendina funkcinius ir nefunkcinius reikalavimus; 3. Parengia ir pateikia testavimo planą; 4. Atlieka komponentų (angl. unit) testavimą, vidinį saugumo testavimą, posistemės vidinį testavimą, sąsajų su kitomis sistemomis testavimą; 5. Vykdo kuriamos posistemės demonstracijas, atsižvelgia į išsakytas Perkančiosios organizacijos pastabas; 6. Rengia priėmimo testavimo scenarijus; 7. Parengia vidinio testavimo ataskaitą; 8. Patikslina detalios analizės ir projektavimo dokumentaciją (jei reikia). Perkančioji organizacija: 1. Suteikia reikalingą informaciją; 2. Parengia gamybinę ir testavimo aplinkas turimoje infrastruktūroje; 3. Dalyvauja posistemės demonstracijose, teikia atsiliepimus; 4. Peržiūri ir įvertina vidinio testavimo rezultatus;	1. Parengtas ir suderintas diegimo į testinę aplinką planas; 2. Parengtas ir suderintas testavimo planas; 3. Parengta testavimo aplinka Perkančiosios organizacijos infrastruktūroje; 4. Atlikta kuriamos posistemės demonstracija; 5. Pateikta vidinio testavimo ataskaita, kurioje aprašyti atlikto vidinio saugumo testavimo rezultatai ir vidinio testavimo rezultatai (apimtis, vykdymo metodika, testavimo tipai, procedūra, įėjimo/išėjimo kriterijai, testavimo aplinka), pateikiant informaciją apie posistemės sritis, į kurias reikia atkreipti papildomą dėmesį testavimo metu; 6. Parengta programinė įranga diegimui; 7. Pagal poreikį atnaujinta detalios analizės ir projektavimo dokumentacija.	Pagal suderintą darbų atlikimo grafiką. Vidinio testavimo ataskaita turi būti pateikta bent prieš 5 darbo dienas iki diegimo testavimo aplinkoje etapo pradžios. Kuriamos posistemės demonstracijos turi būti vykdomos nuolatos, pagal atskirai suderintą grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
	5. Teikia pastabas ir rekomendacijas.		

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Diegimas į testavimo aplinką	Teikėjas: 1. Parengia ir pateikia programinę įrangą tinkamą įdiegimui Perkančiosios organizacijos testavimo aplinkoje; 2. Konsultuoja Perkančiąją organizaciją diegimo į Perkančiosios organizacijos testavimo aplinką klausimais; 3. Parengia duomenų užkrovimo skriptus į Perkančiosios organizacijos testinę aplinką; 4. Rengia priėmimo testavimo scenarijus, testavimo metodiką ir planą; 5. Parengia naudotojų ir administratorių instrukcijas. Perkančioji organizacija: 1. Peržiūri ir įvertina diegimo planą; 2. Suteikia reikalingą informaciją; 3. Kontroliuoja testavimo aplinką; 4. Peržiūri ir įvertina testavimo planą. 5. Įdiegia pateiktą programinę įrangą į Perkančiosios organizacijos testavimo aplinką. Duomenų teikėjai/gavėjai: 1. Peržiūri ir įvertina testavimo planą.	1. Parengta programinė įranga diegimui į Perkančiosios organizacijos testavimo aplinką; 2. Programinė įranga įdiegta Perkančiosios organizacijos testavimo aplinkoje; 3. Parengti integracinio testavimo scenarijai; 4. Parengti duomenys testavimui (SQL ir/arba kitų skriptų pavidalu); 5.Parengtas bei suderinas su Perkančiąja organizacija ir duomenų teikėjais/gavėjais testavimo planas; 6.Parengti priėmimo testavimo scenarijai, testavimo metodika ir planas; 7. Parengti naudotojų vadovai ir administratorių instrukcijos.	Diegimo etapas turi būti baigtas iki priėmimo testavimo etapo pradžios pagal suderintą darbų grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Integracinis testavimas	Teikėjas: 1. Atlieka testavimą su duomenų teikėjais ir gavėjais Perkančiosios organizacijos testinėje aplinkoje; 2. Atlieka koregavimą pagal pateiktas pastabas bei ištaiso klaidas; 3. Sukuria visą projekto techninę dokumentaciją; 4. Parengia testavimo ataskaitą. Perkančioji organizacija: 1. Suteikia reikalingą informaciją; 2. Registruoja testavimo metu Perkančiosios organizacijos nustatytas klaidas; Vykdo testavimo metu nustatytų problemų šalinimo kontrolę.	1.Integracinio testavimo ataskaita. Integracinio testavimo ataskaitoje turi būti įvertinti integracinio testavimo metu nustatyti defektai, pateiktas jų išsprendimo būdas ir statusas; 2.Sukurta visa techninė dokumentacija; 3.Sukurti analizės ir projektavimo dokumentai, diegimo instrukcijos, projekto surinkimo ir kompiliavimo instrukcijos; 4.Sukurtos vartotojų ir administratorių instrukcijos; 5.Parengtos Klaidų šalinimo ataskaitos.	Integracinio testavimo etapas turi būti baigtas iki Diegimo į gamybinę aplinką pradžios pagal suderintą darbų grafiką.

Priėmimo testavimas	Teikėjas: 1. Parengia naudotojų vadovus ir administravimo instrukcijas. 2. Remiantis parengtais ir suderintais naudotojų vadovais papildo nauja informacija ESPBI IS pagalbos sistemą; 3. Vykdo priėmimo testavimą; 4. Šalina užfiksuotus trūkumus (klaidas); 5. Atlieka reikiamus pakeitimus atsižvelgiant į atsparumo įsilaužimams ir našumo testavimo rezultatus; 6. Parengia priėmimo testavimo ataskaitą; 7. Parengia testavimo scenarijus. Perkančioji organizacija: 1. Teikia pastabas priėmimo testavimo planui ir testavimo scenarijams; 2. Vykdo priėmimo testavimą pagal testavimo plane apibrėžtą testavimo plane apibrėžtą testavimo metodiką ir testavimo scenarijus; 3. Atrinktas nepriklausomas Teikėjas vykdo saugumo testavimą pagal šios techninės specifikacijos apibrėžtas testavimo metodikas ir testavimo scenarijus; 4. Priima programinę įrangą bandomajai eksploatacijai.	1. Sėkmingai atliktas priėmimo testavimas. 2. Atlikti reikiami pakeitimai atsižvelgiant į atsparumo įsilaužimams ir našumo testavimo rezultatus. 3. Parengti naudotojų vadovai ir administravimo instrukcijos. 4. Parengta priėmimo testavimo ataskaita. 5. Priimta programinė įranga bandomajai eksploatacijai.	Priėmimo testavimas turi būti atliktas iki bandomosios eksploatacijos pradžios pagal suderintą darbų atlikimo grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Diegimas į gamybinę aplinką	Teikėjas: 1. Parengia diegimo į gamybinę aplinką planą; 2. Parengia ekploatacijos pradžios planą; 3. Parengia ir pateikia programinę įrangą tinkamą įdiegimui Perkančiosios organizacijos gamybinėje aplinkoje; 4. Parengia duomenų užkrovimo skriptus į Perkančiosios organizacijos gamybinę aplinką; 5. Parengia ir suderina Bandomosios eksploatacijos planą; 6. Patikslina naudotojų ir administratorių instrukcijas. Perkančioji organizacija: 1. Peržiūri ir įvertina diegimo planą; 2. Suteikia reikalingą informaciją; 3. Vadovauja naujo funkcionalumo paleidimui; 4. Peržiūri ir įvertina bandomosios eksploatacijos planą; 5. Įdiegia pateiktą programinę įrangą į gamybinę aplinką; 6. Kontroliuoja gamybinę aplinką.	1. Parengta programinė įranga diegimui į gamybinę aplinką; 2. Programinė įranga įdiegta gamybinėje aplinkoje; 3. Parengti duomenys gamybinei ekploatacijai (SQL ir/arba kitų scriptų pavidalu); 4. Parengtas ekploatacijos pradžios planas; 5. Suderintas naujo funkcionalumo paleidimo planas su visais duomenų gavėjais/teikėjais; 6. Atliktas naujo funkcionalumo paleidimas. Per nustatytą laiko tarpą sistema parengta eksploatacijai. 7. Diegimo dokumentacija: 7.1. Diegimo aprašai, kuriuose turi būti pateikta: 7.1.1. Realizuotų sprendimų apibendrinantis aprašymas; 7.1.2. Parengti duomenų struktūrų, atributų, duomenų mainų aprašai; 7.1.3. Techninės realizacijos aprašymas (apimantis reikalavimų techniniam sprendimui detalizaciją, Sistemos plėtimo galimybes; 7.1.4. Kita aktuali informacija; 8. Išeities tekstai (jeigu perduodama) ir detali projekto surinkimo instrukcija; 9. Diegimo planas, apimantis: 9.1. Diegimo dalyvių atsakomybes; 9.2. Diegimo veiklų aprašymą; 9.3. Diegimo veiklų grafiką; 9.4. Diegimo schemą.	Šis diegimas gali vykti tik po sėkmingai įvykusio priėmimo testavimo. Šis diegimo etapas turi būti baigtas per 1 (vieną) savaitę nuo priėmimo testavimo etapo pabaigos ir baigtas iki bandomosios eksploatacijos pradžios.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Mokymai (jei reikia)	Teikėjas: 1. Parengia mokymo aplinką (jeigu tokia reikalinga); 2. Vykdo apmokymus. Perkančioji organizacija: 1. Užtikrina mokymo dalyvių dalyvavimą Teikėjo organizuojamuose mokymuose. 2. Vykdo mokymų kontrolę.	1. Mokymų dokumentacija (įskaitant, bet neapsiribojant, detaliai aprašyta skyriuje 6.4.6): 1.1. Mokymų planas; 1.2. Administratorių ir naudotojų vadovai; 1.3. Pagalbos vadovas (angl. Help) (tik elektroniniu formatu); 1.4. Mokymų medžiaga (detalūs reikalavimai skyriuje); 1.5. Parengtos metodinės rekomendacijos duomenų teikėjams ir gavėjams; 2. Įvykdyti mokymai sutartam naudotojų kiekiui; 3. Pateikta mokymų ataskaita.	Pagal suderintą darbų atlikimo grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Bandomoji eksploatacija	Teikėjas: 1. Teikia konsultacijas bandomosios eksploatacijos klausimais; 2. Reaguoja į eksploatacijos metu nustatytus defektus; 3. Užtikrina ekspertų konsultavimą Perkančiosios organizacijos darbuotojams ir IT specialistams; 4. Užtikrina ekspertų konsultavimą Perkančiosios organizacijos darbuotojams ir IT specialistams; 5. Parengia bandomosios eksploatacijos ataskaitą; 6. Užtikrina Sistemos duomenų integralumą ir vientisumą. Perkančioji organizacija: 1. Dirba su parengta sistema; 2. Registruoja bandomosios eksploatacijos metu nustatytas klaidas;	1. Pašalintos bandomosios eksploatacijos metu nustatytos klaidos. Teikėjas bandomosios eksploatacijos metu pagal suderintą klaidų šalinimo grafiką turi šalinti visus suderintos sistemos funkcionalumo trūkumus užregistruotus bandomosios eksploatacijos problemų registre; 2. Bandomosios eksploatacijos dokumentai (įskaitant, bet neapsiribojant, detaliai aprašyta skyriuje 6.4.7): 2.1. Bandomosios eksploatacijos ataskaita. Bandomosios eksploatacijos ataskaitoje turi būti įvertinti bandomosios eksploatacijos metu nustatyti defektai, pateiktas jų išsprendimo būdas ir būsena, pateiktos rekomendacijos dėl tolesnės eksploatacijos; 2.2. Bandomosios eksploatacijos problemų registras.	Pagal suderintą darbų atlikimo grafiką.

Etapas	Atsakomybių aprašymas	Rezultatai/reikalavimai	Terminas
Priėmimas-perdavimas	Teikėjas: 1. Atnaujina techninę dokumentaciją; 2. Įgyvendinus visas paslaugas teikia galutinę sutarties įvykdymo ataskaitą. Perkančioji organizacija: 1. Priima ir tvirtina Teikėjo parengtus rezultatus; 2. Pasirašomas perdavimo-priėmimo aktas; 3. Teikia pastabas Teikėjo pateiktai dokumentacijai ir pasiūlymus tobulinimui.	1. Galutinė sutarties įvykdymo ataskaita; 2. Perdavimo-priėmimo aktas; 3. Sukurta projekto dokumentacija.	Visos paslaugos turi būti suteiktos išskyrus garantinį aptarnavimą.
Garantinė priežiūra	Teikėjas: 1. Parengia garantinės priežiūros reglamentą; 2. Suteikia numatyto laikotarpio garantinį aptarnavimą. Perkančioji organizacija: 1. Dirba su parengta sistema; 2. Registruoja eksploatacijos metu nustatytas klaidas.	1. Suderintas Garantinės priežiūros procedūros dokumentas; Aprašyta skyriuje 6.6 „Reikalavimai garantinei priežiūrai“.	Garantinės priežiūros procedūros dokumentas turi būti pateiktas likus mėnesiui iki Projekto įgyvendinimo pabaigos.

6.4.1. Reikalavimai dokumentacijai ir jos derinimui

Reikalavimo Nr.	Aprašymas
PR-19.	Visa Teikėjo rengiama Projekto dokumentacija turi būti parengta lietuvių kalba vadovaujantis bendrinės lietuvių kalbos taisyklėmis (išskyrus techninius dokumentus, kuriuose informacija gali būti pateikiama anglų kalba), iliustruoti schemomis, lentelėmis, grafikais bei kitomis vaizdinėmis priemonėmis, pateikiama medžiaga išdėstoma aiškiai, nuosekliai ir detaliai.
PR-20.	Teikėjo pataisyti dokumentai turi būti teikiami su matomais pakeitimais („track changes“ funkcija).
PR-21.	Su Perkančiąja organizacija suderinti dokumentai turi (gali) būti keičiami vėlesnių etapų metu, jeigu yra vykdomi modifikuojamos Sistemos pakeitimai, atsižvelgiant į priėmimo testavimo bei bandomosios eksploatacijos rezultatus, kitas projekto veiklas ir aplinkybes, kurios susijusios su pateiktos dokumentacijos turiniu. Projekto dokumentacija turi būti aktualizuojama (atnaujinama) ir galutinės versijos pateiktos su Perkančiąja organizacija suderintais terminais bet ne vėliau kaip iki galutinio priėmimo perdavimo akto pateikimo dienos.
PR-22.	Dokumentų galutinės versijos turi būti pateiktos Confluence, MS Word arba kitu su Užsakovu suderintu redagavimui tinkamu formatu įkeliant dokumentą (-us) į suderintą direktoriją.
PR-23.	Preliminarios (projektinės) versijos turi būti pateikiamos elektroniniu formatu elektroninio ryšio priemonėmis. Pastabos bei korekcijos dokumentų projektuose turi būti teikiamos Confluence, MS Office programinio paketo (ar lygiaverčio) pakeitimų sekimo (angl. track changes) bei komentavimo funkcijomis. Turi būti vykdomas pateikiamų dokumentų versijavimas (versijų kontrolė).
PR-24.	Teikėjas turės parengti dokumentaciją, nurodytą 4-oje lentelėje „Paslaugų įgyvendinimo etapai“.
PR-25.	Visi Teikėjo parengti dokumentai turės būti suderinti su Perkančiąja organizacija ir Techninės priežiūros paslaugų teikėju. Detalūs dokumentų derinimo principai ir terminai turės būti pateikti ir suderinti Teikėjo parengtame Paslaugų teikimo reglamente.
PR-26.	Dokumentų galutinės versijos turi būti pateiktos dviem formatais: redagavimui tinkamu elektroniniu (.doc, .docx, .pdf arba kitu su Perkančiąja organizacija suderintu formatu) ir Teikėjo atsakingo asmens parašu (elektroniniu arba įprastu) pasirašytu formatu. Dokumentų tarpinės versijos teikiamos tik elektroniniu formatu.
PR-27.	Visa Teikėjo parengta Projekto dokumentacija turi būti patvirtinta Perkančiosios organizacijos atsakingų asmenų, detaliau aprašyta Darbo reglamente.
PR-28.	Perkančioji organizacija ir kitos suinteresuotos šalys pateikia pastabas vertinamai dokumentacijai: 1. ne ilgiau kaip per 10 darbo dienų iki 100 psl. apimties dokumentams; 2. per su Teikėju suderintą laikotarpį, kuris ne mažesnis nei 10 darbo dienų, didesniems nei 100 psl. apimties dokumentams; 3. Perkančiąja organizacijai ar kitoms suinteresuotoms šalims pateikus pastabas vertinamai dokumentacijai, Teikėjas turi atlikti taisymus atsižvelgdamas į šiuos reikalavimus:

	i. iki 100 psl. apimties dokumentai turi būti taisomi ne ilgiau kaip per 5 darbo dienas; ii. didesni nei 100 psl. apimties dokumentai turi būti taisomi ne ilgiau kaip per 10 darbo dienų. Sistemos išeities kodų laikymui turi būti naudojama Perkančiosios organizacijos kodo saugykla – GitLab.

6.4.2. Reikalavimai analizei ir projektavimui

Reikalavimo Nr.	Aprašymas
PR-29.	Teikėjas analizės ir projektavimo etapų vykdymo metu turi atlikti detalią veiklos procesų ir poreikių analizę bei projektavimą ir parengti detalios reikalavimų analizės ir projektavimo dokumentus, kurie detalizuoti RPO skyriuje 6.4.1 „Reikalavimai dokumentacijai ir jos derinimui“.
PR-30.	Detalios reikalavimų analizės dokumente turi būti pateikti pagal Techninės specifikacijos funkcinius ir nefunkcinius reikalavimus bei pagal Perkančiosios organizacijos išsakytus poreikius parengti panaudos atvejai (angl. Use Case) (panaudos atvejų diagramos ir detalūs panaudos atvejų aprašymai, nurodant žingsnius (pagrindinę eiga, alternatyvią eigą, išimtinę eigą) ir kitus apribojimus, naudojant UML (angl. Unified Modeling Language) notaciją. Turi būti atliktas visų Techninės specifikacijos funkcinių ir nefunkcinių reikalavimų susiejimas su detalios analizės dokumento turiniu (skyriais, panaudos atvejais, diagramomis ir pan.). Siejimas turi būti atliekamas tokia forma, kad būtų aišku kokiu būdu yra projektuojamas ir realizuojamas kiekvienas RPO reikalavimas.
PR-31.	Atliekant analizę ir projektavimą Teikėjas turi vykdyti susitikimus su Perkančiosios organizacijos paskirtais veiklos specialistais ir kitų susijusių institucijų specialistais.
PR-32.	Detalios analizės ir projektavimo etapų metu Teikėjas turi detalizuoti RPO funkcinius ir nefunkcinius reikalavimus, kad jais vadovaujantis būtų galima realizuoti poreikius atitinkančius Sistemos funkcionalumus.

6.4.3. Reikalavimai demonstracijoms

Reikalavimo Nr.	Aprašymas
PR-33.	Teikėjas vystymo etape po kiekvienos iteracijos pabaigos turi atlikti Sistemos demonstracijas gyvai demonstruojant Sistemos veikimą. Turi būti atliekamas Sistemos demonstravimas, o ne prototipo.
PR-34.	Demonstruojamo funkcionalumo apimtys ir laikiškumas turi būti nustatyti Paslaugų teikimo reglamente. Iki priėmimo testavimo etapo pradžios Perkančiajai organizacijai turi būti pademonstruotas visas Sistemos funkcionalumas, išskyrus tą funkcionalumą, kuris bus suderintas kaip nedemonstruotinas (pavyzdžiui, integracijos).
PR-35.	Demonstracijų tikslas – supažindinti Perkančiąją organizaciją su kuriama programine įranga bei gauti atsiliepimus dėl sukurto (kuriamo) funkcionalumo.

PR-36.	Pastabos (atsiliepimai) gali būti išsakomos pakartotinai priėmimo testavimo etape, jeigu į jas nebus atsižvelgta iki pastarojo etapo.
PR-37.	Demonstracijų metu išsakomi atsiliepimai (pastabos) turi būti registruojami susitikimo protokoluose ar kita sutarta forma (pavyzdžiui, specializuotoje klaidų registravimo ir sekimo sistemoje).
PR-38.	Funkcionalumo demonstraciją turi vykdyti Teikėjo specialistai, o jo metu Perkančiosios organizacijos atstovai, siekdami objektyviai įvertinti Teikėjo demonstruojamų funkcionalumų galimybes, galės užduoti Teikėjui klausimus.
PR-39.	Demonstravimas turi būti atliekamas lietuvių kalba arba su vertimu į lietuvių kalbą. Nebent numatyta kitaip projekto valdymo plane.
PR-40.	Jeigu Teikėjas negalėtų pademonstruoti atitinkamų funkcionalumų dėl techninių kliūčių, demonstracija galėtų būti vieną kartą atidedama 1 darbo dienai, per kurią Teikėjas turėtų pašalinti technines kliūtis ir atlikti demonstraciją;
PR-41.	Funkcionalumas turėtų būti demonstruojamas veikiančioje demonstracinėje aplinkoje, t. y. negalėtų būti pateikiamas vaizdo įrašas ar pan.

6.4.4. Reikalavimai diegimui

Reikalavimo Nr.	Aprašymas
PR-42.	Iki sprendimo diegimo pradžios Teikėjas turi parengti diegimo planą (kuris tvirtinamas Perkančiosios organizacijos), kuriame turi būti pateikiama: 1. Diegimo dalyvių atsakomybės; 2. Diegimo veiklų aprašymai (diegimo instrukcija); 3. Diegimo veiklų grafikas; 4. Diegimo schema.
PR-43.	Diegimo plane turi būti aprašyti ir suderinti sistemos atstatymo veiksmai įvykus nesėkmingam pakeitimų diegimui.
PR-44.	Programinės įrangos diegimas turi būti vykdomas Perkančiosios organizacijos infrastruktūroje tuo metu, kai Sistemos naudojamumas yra mažiausias (pvz.: ne darbo valandomis arba savaitgalį). Konkretus laikas (grafikas) turi būti suderintas su Perkančiaja organizacija.
PR-45.	Diegimo schema turi būti sudaryta laikantis Perkančiosios organizacijos reikalavimų saugumui, greitaveikai, naudojamumui ir kt.
PR-46.	Atlikus diegimą turi būti įsitikinta, kad visi Sistemos komponentai veikia ir yra pasiekiami iš išorinių tinklų, jei tai yra būtina.
PR-47.	Nepriklausomai nuo sprendimo diegimo būdo, Paslaugų teikėjas turi paruošti bendrą Sistemos diegimo paketą (apimantį tiek esamas, tiek modernizuotas ir naujas Sistemos funkcijas), kurį Perkančioji organizacija galėtų įdiegti savarankiškai bet kada pasibaigus Projektui.

6.4.5. Reikalavimai testavimui

Reikalavimo Nr.	Aprašymas
PR-48.	Turi būti atlikti Sistemos versijų testavimai (toliau – Testavimas).

PR-49.	Testavimo tikslai: 1. Įsitikinti, kad yra įgyvendinti visi funkciniai ir nefunkciniai Techninės specifikacijos reikalavimai; 2. Įsitikinti, kad reikalavimų įgyvendinimas atliktas tinkama apimtimi; 3. Nustatyti ar reikalavimų įgyvendinimas tenkina Perkančiąją organizaciją ir kitas suinteresuotas šalis; 4. Identifikuoti, užregistruoti ir ištaisyti funkcionalumo klaidas (angl. Bugs).
PR-50.	Paslaugų teikėjas turi parengti ir su Perkančiąja organizacija suderinti testavimo planą, kuriame turi būti pateikiama: 5. testavimo metodika; 6. testavimo dalyvių atsakomybės; 7. testavimo apimtis; 8. testavimo aplinka; 9. testavimo scenarijų struktūra; 10. testavimo veiklų grafikas; 11. testavimui reikalingi duomenys (sąlygos); 12. testavimo vykdymo ir klaidų bei trūkumų (funkcinių neatitikčių) registravimo ir šalinimo tvarka; 13. testavimo priėmimo kriterijai; 14. kita aktuali informacija.
PR-51.	Turi būti atlikti šie testavimai: 1. Vidinis testavimas. Vidinius atskirų komponentų testavimus Teikėjas turi atlikti nedalyvaujant Perkančiosios organizacijos atstovams, tačiau turi pateikti tokio testavimo įrodymus – vidinio testavimo ataskaitas, automatinių testavimų scriptus (scriptai turi būti įkelti į Perkančiosios organizacijos kodų versijavimo sistemą GitLab) ir nustatytų neatitikimų sąrašą. Vidinis testavimas turi būti atliktas Teikėjo kūrimo aplinkoje. Automatiniai testai turi būti įtraukti į automatinius CI/CD procesus. Vidinio testavimo veiklos turi būti vykdomos pagal suderintą Paslaugų teikimo reglamentą ir Perkančiosios organizacijos testavimo valdymo priemonėje XRAY Teikėjo parengtais testavimo scenarijais. 2. Apkrovos ir našumo testavimas. Šį testavimą Teikėjas turi atlikti savo kūrimo aplinkoje, nedalyvaujant Perkančiosios organizacijos atstovams. Šio testavimo rezultatai turi atsispindėti vidinio testavimo ataskaitoje. Perkančiosios organizacijos testavimo aplinkoje bus vykdomi papildomi apkrovos ir našumo testavimai. Jei Perkančiosios organizacijos atlikti testavimo rezultatai netenkins nurodytų reikalavimų, Teikėjas turės atlikti reikiamas sistemos optimizavimo veiklas; 3. Integracinis testavimas (angl. Integrity Testing). Šį testavimą Teikėjas turi atlikti TEST aplinkoje su Perkančiosios organizacijos atstovais. Šio testavimo rezultatai būtini įsitikinti ar Sistemos vystymo sprendimas parengtas diegimui į PROD aplinką. Šio testavimo metu rastos klaidos ir neatitikimai turi būti pašalinti ir ištaisyta Sistemos versija sėkmingai ištestuota TEST aplinkoje;

	4. Priėmimo testavimas (angl. Acceptance Testing). Šis testavimas turi būti atliekamas TEST aplinkoje dalyvaujant Teikėjui, Perkančiąja organizacijai ir kitoms suinteresuotoms šalims: a. Šio testavimo metu turi būti tikrinamas testavimo tikslų įgyvendinimas (įgyvendinimo lygio nustatymas). Priėmimo testavimo veiklos turi būti vykdomos remiantis priėmimo testavimo planu, kurį pateiks Teikėjas, priėmimo testavimo scenarijais parengtais Teikėjo Perkančiosios organizacijos testavimo valdymo priemonėje XRAY; Atliktas testavimas turi užtikrinti, kad Sistemos versija yra tinkama bandomajai eksploatacijai; b. Testavimo metu turi būti vykdomas identifikuotų klaidų (problemų) registravimas elektronine forma vedamajame pastebėtų klaidų (problemų) ir jų būsenų kaupimo žurnale. Jei nebus sutarta kitaip, klaidos turi būti registruojamos Perkančiosios organizacijos įrankyje JIRA; c. Kai paslaugos teikimas apima ir testavimo (nepriklausomai nuo aplinkos) veiksmus, Teikėjas, teikdamas paslaugą, turi užtikrinti (naudoti) testavimui reikalingus išteklius (testinius duomenis, įskaitant asmens duomenis, kai testavimo negalima atlikti su sintetiniais (nerealiais) asmens duomenimis); d. Priėmimo testavimas turi būti vykdomas Perkančiosios organizacijos įsigytos techninės įrangos pagrindu; e. Teikėjas turės parengti ir pateikti visus testavimui reikalingus duomenis, įrankius ar kitas priemones; f. Teikėjas turės sudaryti ir kitus testavimo duomenis, kurie bus reikalingi tam, kad patikrinti šių RPO funkcinius ir nefunkcinius reikalavimus. Kiti reikalingi testavimo duomenys, reikiamos priemonės ir sąlygos turi būti detalizuotos priėmimo testavimo plane bei suderintos su Perkančiąja organizacija; g. Priėmimo testavimas užbaigiamas, kai tenkinami testavimo plane įvardinti testavimo priėmimo kriterijai; h. Atliktas testavimas turi užtikrinti, kad Sistemos versija yra tinkama bandomajai eksploatacijai.
PR-52.	Teikėjas turės parengti pačios Sistemos ir ją sudarančių komponentų automatizuoto testavimo ir diegimo (angl. Continuous Integration and Delivery (toliau - CI/CD)) procesus Perkančiosios organizacijos naudojamoje priemonėje GitLab.
PR-53.	Teikėjo su Perkančiąja organizacija suderinti ir sudaryti CI/CD procesai (angl. Pipeline) turi užtikrinti: 1. Artefaktų pagaminimą; 2. Artefaktų ir kodo kokybės patikrinimą; 3. Artefaktų ir kodo saugumo patikrinimą (Perkančioji organizacija pateiks įrankius reikalingus kodo saugumui patikrinti);

	4. Automatinį testų vykdymą; 5. Diegimą į testavimo aplinką; 6. Diegimą į bandomosios eksploatacijos aplinką; 7. Diegimą į gamybinę aplinką.
PR-54.	Perkančioji organizacija savo iniciatyva gali atlikti bet kokius kitus Sistemos testavimus ir bandymus (išeities kodų tikrinimą, konfigūracijos tikrinimą, našumo tikrinimą, aukšto prieinamumo tikrinimą, plečiamumo tikrinimą, funkcionalumo tikrinimą ir kt.) siekdama užtikrinti sistemos kokybę ir atitikimus reikalavimams. Teikėjas turės atsižvelgti į Perkančiosios organizacijos atstovų atliktų bandymų ir testavimų rezultatus, fiksuotus JIRA sistemoje, atlikti visų testavimų rezultatuose nurodytų trūkumų (pažeidimų, rekomendacijų) šalinimą. Teikėjas turės sudaryti reikiamas sąlygas suplanuotiems testavimams ir bandymams atlikti – pateikti išeities kodą, pateikti prisijungimo duomenis prie sistemos komponentų, sukurti testavimui reikalingus naudotojus, įjungti / išjungti sistemos komponentus, sudaryti prieigos galimybes specializuotai testavimo ir bandymų programinei įrangai, atlikti kitas reikiamas veiklas, kurios užtikrintų pilnavertį testavimų ir bandymų proceso įvykdymą.

6.4.6. Reikalavimai mokymams

Reikalavimo Nr.	Aprašymas
PR-55.	Teikėjas turi parengti ir suderinti su Perkančiąja organizacija mokymo planą, mokymų medžiagą bei parengti mokymams reikalingą aplinką.
PR-56.	Mokymų medžiaga turi apimti: 1. atskiroms naudotojų grupėms skirtus naudojimosi funkcionalumais aprašus (paremtus naudotojų instrukcijomis); 2. animuotas naudojimosi instrukcijas ir/ arba vaizdinę (video) medžiagą, leidžiančią organizuoti mokymus atskiroms naudotojų grupėms nuotoliniu būdu.
PR-57.	Mokymų medžiaga turi atitikti tokius reikalavimus: 1. visa pateikta medžiaga turi būti suskirstyta pagal sukurtos programinės įrangos funkcines sritis, parengta lietuvių ir anglų kalbomis ir iliustruota naudotojo sąsajos ekranvaizdžiais; 2. vadovai turi būti išsamūs ir suprantami skaitytojui savarankiškai vykdant konkrečias užduotis, apimti visas numatytas sistemos funkcijas; 3. vadovuose turi būti pateikti visų sukurtos programinės įrangos laukų paaiškinimai; 4. administratorių vadove, turės būti pateikiamas išsamus duomenų importo iš kitų sistemų aprašymas.
PR-58.	Mokymų medžiaga turi būti patalpinta su Perkančiąja organizacija suderintose vietose/direktorijose ir pasiekiama po Projekto.
PR-59.	Mokymai turi būti vykdomi testinėje ar kitoje specialiai mokymams parengtoje aplinkoje.
PR-60.	Perkančiosios organizacijos naudotojų mokymams turi būti apmokyti ne daugiau kaip 20 asmenų.

PR-61.	Naudotojų mokymų vietą turi parinkti Teikėjas prieš tai suderinęs su Perkančiąja organizacija (suderinus mokymai galės būti vykdomi ir nuotoliniu būdu). Su mokymų vieta susijusios išlaidos yra Teikėjo atsakomybė.

6.4.7. Reikalavimai bandomajai eksploatacijai

Reikalavimo Nr.	Aprašymas
PR-62.	Turi būti atlikta Sistemos bandomoji eksploatacija, kurios tikslas – užtikrinti Sistemos kokybę, išbandyti gamybinę sistemos komponentų konfigūraciją, identifikuoti ir pašalinti bandomosios eksploatacijos metu pastebėtus defektus, stabilizuoti darbinės aplinkos konfigūraciją, atsižvelgiant į bandomosios eksploatacijos metu sukauptą patirtį.
PR-63.	Iki bandomosios eksploatacijos pradžios Paslaugų teikėjas turi parengti bandomosios eksploatacijos planą, kuriame turi būti pateikiama: 1. bandomosios eksploatacijos dalyvių komunikavimo schema; 2. bandomosios eksploatacijos dalyvių atsakomybės; 3. bandomosios eksploatacijos veiklų grafikas; 4. bandomosios eksploatacijos vykdymo ir klaidų bei trūkumų registravimo ir šalinimo tvarka; 5. bandomosios eksploatacijos priėmimo kriterijai.
PR-64.	Teikėjas, turi konsultuoti Perkančiąją organizaciją bandomosios eksploatacijos aplinkos parengimo klausimais: 1. sistemos komponentų instaliavimo ir konfigūravimo; 2. visų būtinų sistemos duomenų migravimo (suvedimo) bei perteklinių (bandomajai eksploatacijai nereikalingų) duomenų pašalinimo.
PR-65.	Perkančioji organizacija užtikrina sistemos veikimą visos bandomosios eksploatacijos metu, jeigu nebus sutarta kitaip.
PR-66.	Bandomosios eksploatacijos metu turi būti vykdomas identifikuotų klaidų (problemų) registravimas ir šalinimas: 1. klaidos turi būti registruojamos Perkančiosios organizacijos klaidų sekimo įrankyje – JIRA; 2. Teikėjas privalo nedelsiant per bandomosios eksploatacijos plane numatytus terminus pašalinti sistemos trūkumus atsižvelgiant į užregistruotas bandomosios eksploatacijos problemų registre klaidas.
PR-67.	Pasibaigus bandomajai eksploatacijai Paslaugų teikėjas turi parengti bandomosios eksploatacijos ataskaitą, kurioje būtų pateikta rastų ir ištaisytų klaidų suvestinė, pateikiama informacija apie kitas bandomosios eksploatacijos metu įgyvendintas veiklas.
PR-68.	Perkančioji organizacija pradės Sistemos priėmimo veiklas tik tada, kai Sistema tenkins bandomosios eksploatacijos plane apibrėžtus priėmimo kriterijus.

6.5. Reikalavimai Sistemos priėmimui

Reikalavimo Nr.	Aprašymas

PR-69.	Galutinis Sistemos ar atskirų Sistemos komponentų priėmimas bus vykdomas pasibaigus bandomajai eksploatacijai, t. y. priėmimas galės būti vykdomas tik tada, kai bus pasiekti bandomosios eksploatacijos priėmimo kriterijai.
PR-70.	Teikėjas privalo prieš priduodamas Sistemą Perkančiąja organizacijai pateikti galutines dokumentacijos ir Sistemos išeities kodo versijas, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus, jeigu jos buvo pakeistos nuo paskutinio pridavimo.
PR-71.	Visos Paslaugas bus priimami pasirašant galutinį priėmimo-perdavimo aktą.
PR-72.	Siekiant užtikrinti sklandų Pirkimo tęstinumą: 1. Teikėjas, nepažeidžiant autoriaus teisių turėtojo ar trečiųjų šalių intelektinės nuosavybės teisių, sutartimi perduoda Perkančiąja organizacijai autorių turtines teises į pagal užsakymą sukurtą programinę įrangą ir parengtus projektinius dokumentus, įskaitant, bet neapsiribojant, teisę neribotą laiką ir be papildomo atlygio naudoti sukurtą programinę įrangą; teisę daryti sukurtos programinės įrangos kopijas; teisę modifikuoti ir toliau plėtoti sukurtą programinę įrangą; teisę perkelti programinę įrangą į kitą technologinę platformą; teisę naudoti ir keisti jai sukurtos programinės įrangos pradinį kodą (mašininės kalbos pradinius tekstus); 2. jeigu Projekte sukurtoje programinėje įrangoje panaudota kita autoriaus teisių turėtojo ar trečiųjų šalių programinė įranga, kuri integruota į pagal užsakymą sukurtą programinę įrangą ar kitaip susieta su atliktu užsakymu ir autoriaus turtinių teisių į sukurtą programinę įrangą ar parengtus projektinius dokumentus, jos perdavimas Perkančiąja organizacijai neturi apriboti šias teises perdavusio Teikėjo teisės be atskiro Perkančiosios organizacijos sutikimo toliau vystyti, tobulinti, platinti ir atlikti kitus reikiamus veiksmus su sukurta programine įranga ar parengtais projektiniais dokumentais; 3. kartu su kompiuterine programa, kaip ši sąvoka apibrėžta LR autorių teisių ir gretutinių teisių įstatyme, Perkančiąja organizacijai perduodamas ir programos išeities kodas, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus. Kompiuterių programos autoriaus asmeninės neturtinės teisės negali būti naudojamos tokiu būdu, kuris suvaržytų autorių turtinių teisių į šią kompiuterinę programą turėtojo teises, tarp jų ir teisę savo nuožiūra adaptuoti, keisti ir neatlygintinai platinti šiuos kūrinius. Šiame punkte numatytos autorių turtinės teisės, vadovaujantis Autorių teisių ir gretutinių teisių įstatymo ir Valstybės informacinių išteklių valdymo įstatymo 12 str. nuostatomis, perduodamos ir suteikiamos LR ir ES šalių teritorijoje neribotam laikui; 4. Teikėjas turi perduoti Perkančiąja organizacijai Pirkimo metu sukurtą Sistemos programinę įrangą ir jos išeities kodą ar atskirų Sistemos komponentų paslaugų priėmimo – perdavimo akto pasirašymo datai; 5. Teikėjas neturi teisės atskleisti jokios su paslaugų teikimu susijusios informacijos trečiosioms šalims be Perkančiosios organizacijos raštiško leidimo arba jei to reikalauja įstatymai.

6.6. Reikalavimai garantinei priežiūrai

Reikalavimo Nr.	Aprašymas
PR-73.	Paslaugų teikėjas po galutinio Paslaugų perdavimo-priėmimo akto pasirašymo dienos turės: 1. suteikti ne trumpesnę kaip 12 mėnesių trukmės garantinę priežiūrą; 2. užtikrinti Sistemos veiklos atkūrimą visiško arba dalinio funkcionavimo sutrikimo atvejais, įskaitant sutrikimus, atsiradusius dėl klaidų standartinėje ir nestandartinėje programinėje įrangoje (išskyrus atvejus atsiradusius dėl Perkančiosios organizacijos kaltės); 3. atstatyti sugadintus programinės įrangos komponentus ir duomenis (išskyrus atvejus, atsiradusius dėl Perkančiosios organizacijos kaltės); 4. nemokamai taisyti sukurtos ar modifikuotos programinės įrangos bei kitų sukurtų ar modifikuotų sprendimų klaidas, netikslumus ir neatitikimus Techninėje specifikacijoje apibrėžtiems reikalavimams, taip pat parengti, ištestuoti ir paruošti diegimui reikalingus atnaujinimus pagal Teikėjo parengtas ir su Perkančiąja organizacija suderintas atnaujinimų diegimo procedūras.
PR-74.	Garantinio aptarnavimo metu Teikėjas privalo registruoti Sistemos eksploatavimo sutrikimus ir neatitiktis problemų / sutrikimų registravimo sistemoje (pvz., specializuotoje interneto svetainėje arba per pagalbos teikimo liniją (angl. Service Desk) pagal su Perkančiąja organizacija suderintas informavimo ir registravimo procedūras.
PR-75.	Garantinio aptarnavimo metu visos atsiradusios ir nustatytos klaidos, trikdžiai, sutrikimai ir problemos turi būti klasifikuojami: 1. Kritinis sutrikimas – kai nustatytas trikdis ir (ar) problema, dėl kurios naudotojas negali vykdyti numatytų būtinų funkcijų ir nežinomas joks kitas Perkančiajai organizacijai priimtinas alternatyvus šios funkcijos vykdymo kelias; 2. Nekritinis sutrikimas – kai nustatytas trikdis ir (ar) problema, kuris sukelia sunkumus naudojantis Sistema, bet neturi įtakos Sistemos funkcijų veikimui ir nedaro jokio kito poveikio.
PR-76.	Pagrindinės privalomos garantinės priežiūros sąlygos: 1. reakcijos į problemą laikas (problema užregistruota ir perduota sprendimui) – ne ilgiau kaip 2 val.; 2. problemos sprendimo trukmė: a. kritinių sutrikimų šalinimas – ne ilgiau kaip 8 valandos nuo pranešimo gavimo sutartu būdu; b. nekritinių sutrikimų šalinimas – ne ilgiau kaip 40 darbo valandų nuo pranešimo gavimo sutartu būdu. 3. jei gedimo per nurodytą laiką pašalinti negalima, kartu su Perkančiąja organizacija suderinamas kitas gedimo pašalinimo laikas, pateikiant šio laiko poreikio pagrindimą.
PR-77.	Konsultacijos dėl nustatytų neatitikimų ir apie atliktus programinės įrangos pasikeitimus telefonu ir elektroniniu paštu (angl. Hot line) – darbo dienomis nuo 8:00 iki 17:00 val.

PR-78.	Galimybė visą parą registruoti problemas internetu bei stebėti problemų sprendimo būklę naudojant Perkančiosios organizacijos naudojamą klaidų registravimo įrankį (nebent projekto metu būtų šalių sutarta naudoti Teikėjo klaidų registravimo įrankį).
PR-79.	Kiekvieno ketvirčio pradžioje Paslaugų teikėjas per 5 darbo dienas turės parengti praėjusio ketvirčio garantinės priežiūros vykdymo ataskaitą.
PR-80.	Detali garantinės priežiūros tvarka (garantinės priežiūros komunikacijos būdai, atnaujinimų diegimo procedūros ir kt.) turi būti suderinta su Perkančiąja organizacija aprašyta Teikėjo parengtame garantinės priežiūros reglamente.

6.7. Reikalavimai Projekto valdymui

Reikalavimo Nr.	Aprašymas
PR-81.	Teikėjas turi užtikrinti, kad visa komunikacija Projekto metu vyktų lietuvių kalba. Jei pasitelkiami užsienio šalių ekspertai, Teikėjas turi pasirūpinti vertimo į lietuvių kalbą paslaugomis savo sąskaita.
PR-82.	Pirkimo paslaugos turi būti įgyvendinamos kompleksiniu projekto įgyvendinimo metodu. Etapų (prieaugių) trukmę ir darbų išskaidymą į prieaugius Teikėjas turi suderinti su Perkančiąja organizacija.
PR-83.	Teikėjas turi informuoti Perkančiąją organizaciją apie Paslaugų vykdymo eigą ir Perkančiosios organizacijos prašymu rengti Paslaugų teikimo etapų rezultatų pristatymus.
PR-84.	Teikėjas turi tiesiogiai bendradarbiauti su Perkančiąja organizacija, Projekto partneriais bei kitomis Projekto suinteresuotomis šalimis.
PR-85.	Teikėjas turi pateikti ir su Perkančiąja organizacija suderinti Paslaugų teikimo reglamentą, kuriame turi būti detalizuoti Paslaugų teikimo etapai ir jų rezultatai (pateiktys), pateiktas detalus Perkančiosios organizacijos nurodytus terminus atitinkantis kalendorinis darbų vykdymo grafikas, aprašytos komunikacijos ir rizikų valdymo priemonės bei dokumentų derinimo tvarka.
PR-86.	Teikėjas turi kas mėnesį rengti ir Perkančiąja organizacijai teikti tarpines Paslaugų teikimo ataskaitas, kuriose būtų pateikiama: 1. informacija apie Paslaugų teikimo sutarties vykdymo eigą; 2. informacija apie per ataskaitinį mėnesį užfiksuotas rizikas ir problemas; 3. informaciją apie suderintus pakeitimus pakeitimų registre.
PR-87.	Tarpinės Paslaugų teikimo ataskaitos Perkančiąja organizacijai privalo būti pateiktos per 5 darbo dienas nuo ataskaitinio laikotarpio pabaigos.
PR-88.	Baigus visus darbus, Teikėjas turi parengti galutinę Paslaugų teikimo ataskaitą. Galutinė ataskaita Perkančiąja organizacijai turi būti pateikta per 10 darbo dienų nuo paskutinio Paslaugų teikimo etapo pabaigos.

6.8. Reikalavimai pakeitimų valdymui

Reikalavimo Nr.	Aprašymas

PR-89.	RPO, Techninėje specifikacijoje ar kituose Paslaugų teikimo sutarties prieduose nustatyti reikalavimai gali būti keičiami Teikėjo ar Perkančiosios organizacijos iniciatyva.
PR-90.	Pakeitimų atsiradimas gali būti sąlygojamas aplinkybių, kurios atsiranda arba tampa žinomos po pirkimo sutarties sudarymo, jų atsiradimo pasiūlymo pateikimo ar pirkimo sutarties sudarymo metu nebuvo galima protingai numatyti ir kontroliuoti, taip pat, iš anksto įvertinti ir jų atsiradimo rizikos.
PR-91.	Pakeitimas turi būti įforminamas Paslaugų teikėjui ir Perkančiajai organizacijai patvirtinus keitimą raštu, vadovaujantis tarp Paslaugų teikėjo ir Perkančiosios organizacijos sudarytos Paslaugų teikimo sutarties ir šios Techninės specifikacijos sąlygomis, nepažeidžiant viešųjų pirkimų principų, esant visoms šioms aplinkybėms: 1. dokumentuotas funkcionalumo pakeitimo poveikis, aprašytas jo kritiškumo laipsnis (neesminis, vidutinis, kritinis) ir pasekmės; 2. funkcionalumo pakeitimas nėra kritinis ir nedaro įtakos viso techninio sprendimo funkcionalumui; 3. funkcionalumo pakeitimas buvo / yra pažymėtas testavimo plane ir bus papildomai ištestuotas; 4. atlikti techninės dokumentacijos, veiklos procesų ir / ar teisės aktų pakeitimai, susiję su funkcionalumo pakeitimu; 5. funkcionalumo pakeitimas yra autorizuotas (pasirašytas Perkančiosios organizacijos įgalioto asmens); 6. apie funkcionalumo pakeitimą yra tinkamai pranešta visoms su Paslaugų teikimu susijusioms šalims; 7. keičiamas funkcionalumas neapsunkina pirkimo tikslų pasiekimo; 8. visi su funkcionalumu susiję pakeitimai yra vedami funkcionalumų pakeitimo registracijos žurnale.
PR-92.	Jeigu funkcionalumo pakeitimas yra įvykdytas nesilaikant ankstesniame punkte nustatytos tvarkos, toks funkcionalumo pakeitimas laikomas negaliojančiu.

6.9. Reikalavimai priežiūros paslaugų teikimui

Reikalavimo Nr.	Aprašymas
PR-93.	Priežiūros paslaugos bus teikiamos gavus Perkančiosios organizacijos užsakymą. Užsakyme bus nurodytas priežiūros paslaugos laikotarpis.
PR-94.	Priežiūros paslaugos pradedamos teikti ne anksčiau nei pasibaigs garantinės priežiūros laikotarpis ir gavus Perkančiosios organizacijos užsakymą.
PR-95.	Priežiūros paslaugos turi būti teikiamos darbo dienomis nuo 8.00 val. iki 17:00 val., o jeigu Sistemos veikimo sutrikimas įtakoja Perkančiosios organizacijos gebėjimą teikti paslaugas – ir kitu laiku.
PR-96.	Teikėjas turi įvertinti, kad Paslaugų teikimo laikotarpiu gali būti vykdomas Sistemos (ar jų duomenis naudojančių komponentų) informacinių technologijų infrastruktūros (tame tarpe ir standartinės programinės įrangos) atnaujinimas ir vystymas, Sistemos modernizavimas.

PR-97.	Jeigu teikiant priežiūros paslaugas yra reikalingas Sistemos techninės dokumentacijos atnaujinimas, ji turi būti atnaujinama. Sistemos naudojimo instrukcijos taip pat turi būti atnaujintos bei pateiktos ir per programinės įrangos naudotojo sąsają (naudotojui suteikiant galimybę pasirinkti naudojimo instrukciją iš programinės įrangos meniu). Dokumentacijos atnaujinimo poreikis turi būti įvertinamas kiekvieną mėnesį.
PR-98.	Esant būtinybei, atstatant Sistemos veiklą priežiūros paslaugos teikiamos ir kitu iš anksto suderintu laiku taip, kad nebūtų pažeisti Perkančiosios organizacijos nustatyti Sistemos atstatymo terminai.
PR-99.	Teikėjas turi paskirti atsakingus už priežiūros paslaugų teikimą asmenis, kurie turi būti pasiekiami registruojant užduotis Perkančiosios organizacijos naudojamoje informacinių technologijų užduočių valdymo ir tvarkymo sistemoje JIRA (toliau — Perkančiosios organizacijos JIRA), nurodytu telefono numeriu ir elektroniniu paštu.
PR-100.	Visas su priežiūra susijusias veiklas paslaugų Teikėjas turės organizuoti taip, kad visos Perkančiosios organizacijos užsakomos paslaugos, Teikėjo suteiktų paslaugų rezultatai, jų aprašymai ir kita susijusi informacija būtų registruojami Perkančiosios organizacijos JIRA. Perkančioji organizacija po Sutarties įsigaliojimo suteiks Paslaugų Teikėjo specialistams prieigą prie sukurto JIRA projekto.
PR-101.	Sistemos stebėsena vykdoma Perkančiosios organizacijos priemonėmis. Po Sutarties įsigaliojimo Teikėjas su Perkančiąja organizacija suderina Sistemos stebėjimo taškus ir informavimo, apie pastebėtus sutrikimus (sutrikimas angl. Issue), bei registravimo tvarką.
PR-102.	Teikėjas turi nedelsdamas fiksuoti Perkančiosios organizacijos JIRA ir / arba suderinta tvarka pranešti Perkančiosios organizacijos paskirtiems atsakingiems asmenims apie pastebėtus arba galinčius įvykti Sistemos veiklos sutrikimus, incidentus (taip pat ir elektroninės informacijos saugos incidentus) ir problemas bei numatomus jų šalinimo terminus.
PR-103.	Sprendimą, kokios svarbos Perkančiosios organizacijos JIRA / Pagalbos tarnyboje registruotas kreipinys, ir vertinimą, ar kreipinys tinkamai išspręstas ir gali būti uždarytas, priima Perkančioji organizacija.
PR-104.	Perkančiosios organizacijos JIRA / Pagalbos tarnyboje Teikėjo atstovai privalės iš karto pranešti apie sutrikimo sprendimo eigą, o suradę sprendimą bei išsprendę problemą, pakomentuoti sprendimą (žr. 5 lentelę).
PR-105.	Laiko tarpas, per kurį Paslaugų teikėjas privalės išspręsti kreipinius, priklausys nuo Teikėjo teikiamų paslaugų ir šiems kreipiniams Perkančiosios organizacijos specialistų suteikto prioriteto pagal sutrikimo įtaką Perkančiosios organizacijos veiklai (žr. 6 lentelę).
PR-106.	Perkančiosios organizacijos nustatyti kreipinių prioritetai Critical, Major nenaudojami testavimo ir kūrimo aplinkose esančioms problemoms. Klaidos tyrimo eigoje nustačius naujas aplinkybes, suderinus laikiną alternatyvų problemos pašalinimo būdą, šalims sutarus kreipinio kategorija gali būti keičiama (mažinama arba didinama), nurodant prioriteto keitimo priežastį.
PR-107.	Teikėjas privalo išspręsti kreipinį (suteikti paslaugą ir pateikti diegimo paketą, jei reikalinga) Perkančiosios organizacijos nustatytais terminais, neįskaičiuojant

	laiko, per kurį kreipinį tikslina ar teikia kitus paaiškinimus Perkančiosios organizacijos specialistai.
PR-108.	Visais kitais atvejais sutrikimai turi būti šalinami per šalių suderintą laiką, o konsultacijos suteikiamos ne vėliau kaip iki paklausimo pateikimo darbo dienos pabaigos, jeigu jis pateiktas elektroninėmis priemonėmis ir iki tos darbo dienos 12 val., visais kitais atvejais ne vėliau kaip iki sekančios darbo dienos pabaigos. Jeigu konsultacijos nepavyksta suteikti telefonu ar elektroninio pašto pagalba.
PR-109.	Jei sutrikimo pašalinti neįmanoma per nustatytą laiką (ar šalių suderintą laiką), Teikėjas privalo apie tai informuoti Perkančiąją organizaciją, pateikti ir suderinti su ja gedimų šalinimo planą ir toliau sutrikimo šalinimo veiksmus vykdyti pagal plane numatytus terminus.
PR-110.	Visas Sistemos programinės įrangos klaidas ir neatitikimus jos techninei dokumentacijai ir užsakymų teikti vystymo paslaugas reikalavimams, dokumentacijos trūkumus, taip pat visus Sistemos darbo sutrikimus ir jų padarinius, kurie atsirado įdiegus teikėjo įvykdytus programinės įrangos pakeitimus, Teikėjas šalina savo sąskaita.
PR-111.	Nustatytais kreipinių sprendimo terminais Teikėjas turės pateikti reikalingus diegimui Sistemos programinę įrangą / diegimo paketus su diegimo instrukcijomis.
PR-112.	Teikėjas turi konsultuoti Perkančiosios organizacijos specialistus ir teikti techninę pagalbą naudojant Perkančiosios organizacijos JIRA priemones, telefoną, elektroninį paštą bei specialistų darbo vietoje: 1. Nesant galimybei suteikti konsultaciją iš karto, Teikėjas turi pateikti atsakymus į konsultacijų paklausimus ne vėliau kaip per 8 (aštuonias) Perkančiosios organizacijos darbo valandas (I - IV 8:00 - 17:00, V - 8:00 15:45), skaičiuojamas nuo konsultacijos paklausimo pateikimo Perkančiosios organizacijos sutrikimų sprendimo sistemoje. Šalių sutarimu šis terminas gali būti pratęstas protingam laikotarpiui. Konsultacijos gali būti teikiamos telefonu, elektroniniu paštu, atvykstant į nurodytą Perkančiosios organizacijos patalpą arba kitais šalių sutartais komunikavimo būdais; 2. Pirminis ir antrinis klientų konsultavimo lygis užtikrinamas Perkančiosios organizacijos, techninės priežiūros klausimai, kurių nepavyksta išspręsti Perkančiajai organizacijai registruojami Perkančiosios organizacijos JIRA, vykdymą priskiriant Teikėjo nurodytam asmeniui.
PR-113.	Sistemos įvykių ir kreipinių valdymas turi būti detaliai aprašytas Teikėjo parengiamajame Paslaugų teikimo reglamente.

5 lentelė. Kreipinių registravimas JIRA

Priežiūros sritis	Įvykis, pranešimas, užsakymas	Tipas JIRA	Label JIRA sistemoje
Taikomoji programinė įranga	Nenumatytas e. paslaugos teikimo sutrikimas, pablogėjimas, arba įvykis, kuris gali sutrikdyti e. paslaugos teikimą. Registrų ir informacinių sistemų veikimo sutrikimas, gedimas ar įvykis, dėl kurio nutrūksta elektroninės paslaugos teikimas arba pablogėja paslaugos kokybė ir kurį būtina pašalinti per nustatytą laiko tarpą. Sutrikęs arba gręsiantis pavojus, kad sutriks Registrų ir informacinių sistemų darbingumas pagal automatinio įrankio, Paslaugų teikėjo ar Paslaugos gavėjo specialisto pastebėtą įvykį. Vienas ar keli pasikartojantys incidentai, turintys didelę įtaką informacinės sistemos/registro veikimui, kuriems būdingi tokie pat požymiai, o priežastis, dėl kurios įvyko incidentas, nėra žinoma ar reikalaujanti gilios analizės. Nepašalinus problemos, incidentai gali kartotis. Greitaveikos sutrikimai. Sutrikimų analizė.	Incidentas (sutrikimo analizei vykdyti)	MedVAIS_Priežiūra_Sutrikimas
		Bug (sutrikimo priežasčiai identifikuoti ir klaidai pašalinti)	
Užsakymas pakeisti programinę įrangą	Veikiančios programinės įrangos funkcionalumo, konfigūracijos ar modifikavimo darbai.	Story	MedVAIS_Priežiūra_Pakeitimas
	Techninės skolos (Technical Debt) pvz. IS kodo optimizavimo darbai, integralumo, patikimumo, saugumo užtikrinimo bei technologinių sprendimų atnaujinimo darbai nekeičiantys sistemos funkcionalumo.	Technical Story	
Konsultavimas	Patarimas ar informacija Registrų centro specialistams dėl programinės įrangos, funkcionalumo, jos veikimo, technologiniais sprendimais, vystymo, tarnybinių stočių, kuriose šios sistemos įdiegtos, administravimo, rezervinių kopijų darymo, atstatymo bei veikimo stebėjimo klausimais, taip pat patarimas ar informacija dėl informacinės sistemos/registro duomenų, jų tvarkymu.	Paslaugos prašymas	MedVAIS_Priežiūra_Konsultavimas

Priežiūros sritis	Įvykis, pranešimas, užsakymas	Tipas JIRA	Label JIRA sistemoje
Duomenų, dokumentų tvarkymo paslauga	Registrų ir informacinių sistemų duomenų išrinkimui reikalingų užklausų parengimas ir duomenų išrinkimas pagal Registrų centro poreikius. Dokumentacijos atnaujinimas.	Task	MedVAIS_Priežiūra_ Paslauga
Teikėjo pasiūlymai	Vykdytojo pasiūlymai techniniais arba funkciniais klausimais: pasiūlymai ir išvados dėl Registrų ir informacinių sistemų vystymo poreikių bei techninės bei technologinės architektūros tobulinimo. Pasiūlymai dėl Paslaugų teikimo pagerinimo ir paslaugų kokybės apibendrinimo ataskaita ir kita svarbi informacija. Sistemų naudotojų pasiūlymų, grįžtamojo ryšio peržiūra, analizė, sprendimų formulavimas.	Task	MedVAIS_Priežiūra_ Pasiūlymas

6 lentelė. Kreipinių prioritetai ir sprendimo laikas

Tipas	Prioritetas	Reakcijos laikas	Sprendimo trukmė nuo pateikimo	Aptarnavimo režimas	Aptarnavimo laikas
Incidentas Bug	Kritinis	Iki 15 min.	Iki 4 val.	24x7	0:00 – 24:00
	Aukštas	Iki 15 min.	Iki 6 val.	24x7	0:00 – 24:00
	Vidutinis	Iki 15 min.	Iki 1 d. d.	8x5	8:00 – 17:00
	Žemas	Iki 15 min.	Iki 3 d. d.	8x5	8:00 – 17:00

7. SPECIALIEJI REIKALAVIMAI PASLAUGŲ TEIKIMUI

7.1. Reikalavimai saugai

7.1.1. Reikalavimai duomenų apsaugai ir informacijos saugumo valdymui

Reikalavimo Nr.	Aprašymas
PR-114.	Duomenų sauga turi būti užtikrinta vadovaujantis Sistemos duomenų saugos nuostatais, asmens duomenų apsauga turi būti užtikrinta remiantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
PR-115.	Teikėjas, teikdamas Paslaugas, turi laikytis ir užtikrinti, kad Paslaugos atitiktų Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos

	Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" nustatytus saugumo reikalavimus.
PR-116.	Po Pirkimo darbų įvykdymo Sistemoje saugomi duomenys turi būti apsaugoti nuo nesankcionuoto priėjimo, naudojimo, pakeitimo, atskleidimo, sunaikinimo ar praradimo.
PR-117.	Teikėjas projektuojant Sistemos turi su Perkančiąja organizacija suderinti, kokias apsaugas ir kuriam Sistemos funkcionalumui naudoti. Sistema turi būti apsaugota nuo šių grėsmių: 1. Siekiant išvengti saugumo spragų ir pažeidžiamumo programinėje neautentifikuotos prieigos; 2. nesankcionuoto naudotojo sesijos perėmimo; 3. nesankcionuoto duomenų perėmimo ar jų įterpimo; 4. žalingo kodo įterpimo (angl. Injection, XSS (Cross-sitescripting)); 5. kitų saugumo pažeidimų, kurių sąrašas skelbiamas Atviro tinklo programų saugumo Pirkimo (angl. The Open Web Application Security Project (OWASP) interneto svetainėje www.owasp.org).
PR-118.	Sutrikus sistemų darbui, sistemos naudotojams turi būti pateikiami atitinkami pranešimai.
PR-119.	Įrangoje, kurią naudojant teikiamos paslaugos, Teikėjas, kurdamas programinę įrangą, turi vadovautis visuotinai pripažintais saugaus kodavimo standartais ir gerąja praktika (angl. The Open Web Application Security Project, OWASP) Secure Coding Practices ar lygiaverte). Kuriama programinė įranga neturi turėti nesankcionuotos prieigos prie duomenų ir kitų saugumo pažeidimų, kurie įvardijami naujausiame OWASP Testing Guide (neapsiribojant „OWASP Top 10" pažeidžiamumais) (https://www.owasp.org) sąraše, The OWASP API Security sąraše ir kt. OWASP parengtose IS saugumo metodikose arba lygiaverčiuose dokumentuose.
PR-120.	Saugumo patikrinimai (grėsmių modeliavimai, išeities kodo pažiūros ir kt. saugaus kodavimo standartuose ir gerojoje praktikoje numatyti saugumo patikrinimai) turi būti vykdomi kiekviename programinės įrangos kūrimo etape, vadovaujantis Elektroninių paslaugų kūrimo metodika, patvirtinta Lietuvos Respublikos susisiekimo ministro 2015 m. spalio 7 d. įsakymu, nustatančią reikalavimus atsparumo įsilaužimui testavimui, kurį turi atlikti nuo elektroninių paslaugų kūrimą vykdančio subjekto (Teikėjo) nepriklausomas paslaugų teikėjas. Atliekant saugumo patikrinimus turi būti remiamasi visuotinai pripažintuose metodikose nurodytais saugumo patikrinimo metodais (OWASP application security verification standard, OWASP Testing Guide, Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), SANS, NIST SP 800-30" ar lygiavertėmis saugumo patikrinimo metodikomis).
PR-121.	Teikėjas turi nedelsiant informuoti apie sutarties vykdymo metu Perkančiosios organizacijos informacinių technologijų infrastruktūroje pastebėtus elektroninės informacijos saugos incidentus, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, informacijos saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, Informacinių sistemų saugumo spragas,

	pažeidžiamumą, kitus svarbius saugai įvykius bei, suderinus su Perkančiąja organizacija, imtis atitinkamų priemonių ir veiksmų siekiant nustatyti elektroninės informacijos saugos incidentų priežastis, išvengti susijusios rizikos. Taip pat pagal kompetenciją vykdyti visus Perkančiosios organizacijos saugos įgaliotinio nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu.

7.1.2. Reikalavimai saugą reglamentuojančių teisės aktų taikymui

Reikalavimo Nr.	Aprašymas
PR-122.	Pagrindiniai saugą (tiek programinės įrangos, tiek duomenų) reglamentuojantys teisės aktai, kuriais turi būti vadovaujamasi kuriant Sistema yra šie: 1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas (BDAR)), saugumo valdymo standartas LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“; 2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; 3. Lietuvos Respublikos kibernetinio saugumo įstatymas; 4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo; 5. Informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“; 6. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“; 7. Duomenų teikimo formatų ir standartų rekomendacijos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. kovo 25 d. įsakymu Nr. T-36 „Dėl Duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo“.

7.1.3. Paslaugų teikimo duomenų saugos reikalavimai

Reikalavimo Nr.	Aprašymas
PR-123.	Informacinių išteklių vystymo ir priežiūros saugumas (saugus kodavimas ir kt. turi būti užtikrintas, kaip reikalaujama Lietuvos standartuose LST EN ISO/IEC 27001 ir LST EN ISO/IEC 27002.
PR-124.	Perkančiosios organizacijos tvarkomų registrų ir informacinių sistemų duomenų saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose, Kibernetinių ir elektroninės informacijos saugos incidentų valdymo tvarkos apraše ir kituose teisės aktuose nustatytus saugumo reikalavimus (ir tais atvejais, jeigu tokie reikalavimai keičiasi arba jų atsiranda po viešojo pirkimo–pardavimo sutarties pasirašymo).
PR-125.	Duomenų sauga turi būti užtikrinama: 1. užtikrinant duomenų vientisumą, prieinamumą ir konfidencialumą; 2. registruojant Sistemos naudotojų atliekamus veiksmus su duomenimis, įskaitant duomenų paiešką ir peržiūrėjimą (nustatytai grupei Sistemos naudotojų turi būti privaloma įvesti sistemoje atliekamų veiksmų priežastį ir /ar teisinį pagrindą; 3. sukuriant priemones, sudarančias galimybes Sistemos administratoriui patikrinti Sistemos naudotojų veiksmus; 4. numatant apsaugos nuo atsitiktinio duomenų ištrynimo (pvz. perspėjimai apie numatomą duomenų ištrynimą) priemones bei duomenų trynimo veiksmo tvirtinimą keliems naudotojams („keturių akių principas“). Šis principas turi būti taikomas veiklos bei administravimo aplikacijose; 5. darbui su komponentais Sistemos naudotojus suskirstant į grupes pagal duomenų tvarkymo pobūdį, kai kuriems iš jų suteikiant specialiąsias teises (roles) atlikti tam tikrus tvarkymo veiksmus. Sistemos naudotojų grupių ir rolių aprašymai turi būti parengti analizės ir projektavimo etape; 6. saugoma informacija negali būti ištrinta jokiais kitais būdais ar aplinkybėmis išskyrus analizės ir projektavimo etapuose numatytais atvejais); 7. Teikėjas turi suderinti failų formatus, kuriuos leidžiama įkelti į Sistemą, ir suderinti juos su Perkančiąja (pvz. neturi būti leidžiama prisegti potencialiai nesaugių, galinčių automatiškai pasileisti (angl. Self-executive) failų).

7.1.4. Reikalavimai auditavimui

Reikalavimo Nr.	Aprašymas
PR-126.	Turi būti vykdomas visų Sistemos komponentų funkcionalumo naudojimo (naudotojų atliekamų veiksmų) ir komponentų veikimo auditavimas.
PR-127.	Turi būti realizuotas audito įrašų tvarkymo komponentas, kuris: 1. gautų ir kauptų Sistemos veikimo bei naudojimo duomenis; 2. realizuotų galimybę atlikti audito įrašų analizę (paiešką, filtravimą pagal įvairius parametrus). Reikalingi analitiniai veiksmai su auditavimo įrašais

	turi būti identifikuoti ir suderinti su Perkančiąja organizacija analizės ir projektavimo etapų vykdymo metu; 3. apsaugotų žurnalinius įrašus nuo nesankcionuoto ar netyčinio pakeitimo bei ištrynimo; 4. vykdytų audito įrašų šalinimą bei archyvavimą pagal nustatytas taisykles, kurios turi būti suderintos analizės ir projektavimo etape; 5. sudarytų galimybę eksportuoti pasirinktus audito įrašus.
PR-128.	Atliekant auditavimo įrašo išsaugojimą duomenų bazėje, turi būti kaupiama: 1. kas atliko veiksmą (vartotojas); 2. kada atliko veiksmą (data, laikas); 3. kokius duomenis peržiūrėjo; 4. kokius duomenis atnaujino; 5. kokius duomenis įterpė; 6. naudotojo IP adresas; 7. kokius duomenis pašalino; 8. kokias paieškos frazes naudojo; 9. kita informacija, nustatyta analizės ir projektavimo etapų metu.
PR-129.	Turi būti audituojami su vidinėmis ir išorinėmis sistemomis integracinėmis sąsajomis siunčiami / gaunami duomenys, išsaugant informaciją: 1. iš kokios sistemos, registro ar duomenų bazės gaunami duomenys; 2. į kokią sistemą, registrą ar duomenų bazę siunčiami duomenys; 3. duomenų gavimo/siuntimo data ir laikas; 4. siųsti / gauti duomenys (jeigu tam yra poreikis); 5. kita informacija, nustatyta detalios analizės ir projektavimo etapu metu.

7.1.5. Reikalavimai rizikų, grėsmių ir pažeidžiamumų valdymui

Reikalavimo Nr.	Aprašymas
PR-130.	Turi būti rizikų, grėsmių ir pažeidžiamumų valdymas: 1. Teikėjas privalo vadovautis pripažintomis saugaus programinės įrangos kūrimo metodikomis, tokiomis kaip ISO/IEC 27034-1 arba lygiavertėmis; 2. Teikėjas privalo užtikrinti, kad visi programinės įrangos kūrime dalyvaujantys darbuotojai susipažinę su saugaus programinės įrangos kūrimo metodikomis; 3. Teikėjas privalo atlikti patikrinimą siekdamas identifikuoti pagrindines Sistemos saugumo rizikas bei saugumo pažeidžiamumus, nurodytus CWE/SANS TOP 25 Most Dangerous Software Errors OWASP 10 Most Critical Web Application Security Risks sąrašuose ir rastas rizikas bei pažeidžiamumus pašalinti. Teikėjas atlikęs patikrinimą ir rizikų/pažeidžiamumų šalinimą turi pateikti deklaraciją, kurioje būtų nurodyta jog po kūrimo darbų įvykdymo Sistemoje nėra CWE/SANS TOP 25 ir OWASP TOP 10 sąrašuose nurodytų rizikų/pažeidžiamumų; 4. Teikėjas privalo pateikti visų, sistemoje naudojamų trečių šalių komponentų sąrašą;

	5. Teikėjas privalo imtis tinkamų veiksmų (angl. Reasonable Effort) užtikrinant, kad trečių šalių komponentai atitinka Perkančiosios organizacijos saugumo reikalavimus.
PR-131.	Priėmimo testavimo etapo metu ar bandomosios eksploatacijos etapo metu (ar kitu sutartu metu) Teikėjas turi sudaryti visas reikiamas sąlygas Perkančiosios organizacijos atstovų specialistams, kurie atliks atsparumo įsilaužimams testavimą. Esant poreikiui Teikėjas turės atlikti konfigūravimo ar programavimo darbus, kurie bus būtini siekiant ištestuoti Sistemos saugumą įvairiais jos naudojimo scenarijais. Teikėjas neturės pateikti jokios programinės ar techninės įrangos, skirtos šio testavimo vykdymui.
PR-132.	Teikėjas turi atlikti reikiamus Sistemos programavimo ir / ar konfigūravimo darbus, atsižvelgiant į Perkančiosios organizacijos atstovų atliktų atsparumo įsilaužimams testavimų rezultatus, kad prieš pradedant eksploatuoti Sistema būtų pašalinti visi nustatyti svarbūs saugumo pažeidžiamumai.

7.1.6. Reikalavimai susiję su nacionaliniu saugumu

Reikalavimo Nr.	Aprašymas
PR-133.	Teikėjo siūlomos paslaugos neturi kelti grėsmės nacionaliniam saugumui. Teikėjas, teikdamas ir pasirašydamas pasiūlymą, patvirtina, kad jo siūlomos paslaugos nekelia grėsmės nacionaliniam saugumui. Perkančioji organizacija Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme nustatyta tvarka kreipsis į Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisiją (toliau – Komisija) dėl ketinamo sudaryti sandorio atitikties nacionalinio saugumo interesams patikros ir tuo atveju, jeigu Komisija pareikalaus pateikti papildomus dokumentus Teikėjas, Teikėjų grupės partneriai, ir jų pasitelkiami subteikėjai privalės juos pateikti.
PR-134.	Teikėjas, Teikėjų grupės partneriai, ūkio subjektai, kurių pajėgumais remiamasi ir jų pasitelkiami subteikėjai neturi turėti interesų, galinčių kelti grėsmę nacionaliniam saugumui. Perkančioji organizacija, Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme nustatyta tvarka, kreipsis į Komisiją dėl ketinamo sudaryti sandorio atitikties nacionalinio saugumo interesams patikros ir tuo atveju, jeigu Komisija pareikalaus pateikti papildomus dokumentus Teikėjas, Teikėjų grupės partneriai, ir jų pasitelkiami subteikėjai privalės juos pateikti.
PR-135.	Techninės ar programinės įrangos priežiūra ar palaikymas negali būti vykdomas iš šio Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).
PR-136.	Techninės ar programinės įrangos gamintojas ar jį kontroliuojantis asmuo negali būti registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose (https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/16f99e01af6811ecaf79c2120caf5094).

7.1.7. Kiti saugos reikalavimai

Reikalavimo Nr.	Aprašymas
PR-137.	Projekto įgyvendinimo metu turės būti išlaikomos visos ESPBI IS šiuo metu naudojamos saugumo ir privatumo priemonės.
PR-138.	Teikėjas Sistemos kūrimui turi naudoti naujausias stabilias programinės įrangos versijas ir jos pataisymus (angl. Patch / Fix). Sistemos įdiegimo į PROD aplinką etapo metu turi būti užtikrinta, kad Sistema naudojamos naujausios stabilios PĮ versijos, jeigu tai nekeičia esminių Sistemos architektūros ir funkcionalumo principų, kurie numatyti Projektavimo etape. Neturi būti naudojamos programinių komponentų versijos, kurios yra testavimo stadijoje arba yra oficialiai programinės įrangos gamintojo paskelbta, kad programinė įranga nuo tam tikros datos nebebus palaikoma, tobulinama ir / ar vystoma (angl. End-of-life product).
PR-139.	Sistemoje draudžiama bet kokia neautorizuota ar nedokumentuota nuotolinė ar lokali prieiga/ paskyros ar bet koks slaptas (nedokumentuotas) funkcionalumas galintis pažeisti sistemos saugumą.
PR-140.	Saugi konfigūracija: 1. Teikėjas privalo pateikti detalias sistemos ir platformos (OS, DBMS, Middleware) saugumo konfigūravimo instrukcijas; 2. Sistemos Teikėjas privalo pateikti sistemos funkcionavimui būtinų platformos komponentų, sisteminių paslaugų, prievadų sąrašą. Visi nebūtini Sistemos funkcionalumui komponentai turi būti deaktyvuoti prieš pradedant sistemos eksploataciją.
PR-141.	Duomenų srautai tarp skirtingų lygių turi būti dokumentuoti, nurodant reikalingus komunikacijai prievadus ir protokolus, bei ribojami ugniasienių
PR-142.	Sistema turi būti prieinama naudojantis vieningomis ESPBI IS Saugos posistemės teikiamomis saugos priemonėmis, vieningo prisijungimo (angl. Single Sign On - SSO) principu.
PR-143.	Visa identifikavimo informacija turi būti saugoma šifruotu pavidalu tokiu būdu, kad iš saugomos informacijos būtų neįmanoma atkurti pirminių duomenų (pavyzdžiui, slaptažodžių).
PR-144.	Teikėjas įsipareigoja pateikti Sistemą, kurioje nėra jokių paslėptų, saugumą silpninančių funkcijų, įskaitant: kenksmingos programinės įrangos, virusų, „kirminų", „laiko minų", neautorizuotų prieigų ar funkcijų (Trojans, backdoors, easter eggs).
PR-145.	Integracinių sąsajų pranešimai turi būti šifruojami pasirašomi SHA256 skaitmeniniu parašu.
PR-146.	Sesijų valdymui naudoti HTTP Cookie metodą arba POST užklausas su paslėptais laukais (ang. hidden field).
PR-147.	Sistema turi generuoti sisteminius žurnalus apie naudotojų prisijungimus, prieigos bandymus ir duomenų srautą, kad būtų galima stebėti ir reaguoti į galimus saugumo incidentus.
PR-148.	Nuorodos turi būti šifruojamos naudojant stiprius šifravimo algoritmus (pvz. AES-256).

8. PRIEDAI

8.1.1 priedas. Papildomų paslaugų užsakymo forma

1 priedas

PAPILDOMŲ PASLAUGŲ UŽSAKYMAS

(MedVAIS modernizavimo paslaugos. I dalis)

Sutarties numeris:		Užsakymo pateikimo data:	
Užsakymo numeris:		Numatomas atlikimo terminas:	
Užsakymo pavadinimas:		Numatomos laiko sąnaudos:	

Perkančiosios organizacijos dalis. Paslaugos užsakymo aprašas.

Priedai prie aprašo	□ Yra	Pridedamų lapų skaičius:

Paslaugų teikėjo dalis. Užsakymo realizavimo aprašas.

Perkančiosios organizacijos atsakingas asmuo _____
(vardas, pavardė, parašas)

Paslaugų teikėjo atsakingas asmuo _____
(vardas, pavardė, parašas)

TENDER BID FOR
Purchase and implementation of a complex solution for the modernization of MedVAIS

Part I of the Contract

May 26th, 2025
Vienna-Austria

To the State Enterprise Centre of Registers

1. INFORMATION ABOUT THE TENDERER

Name(s), legal entity code(s) of the tenderer or participants of the group of economic operators *(if the tender bid is submitted by a natural person – No. of Business Licence or Individual Activity Certificate, or similar document), address(-es)*	J4Care GmbH (registration FN 298641d, commercial court Wiener Neustadt (Vienna, Austria))
Collegial management and/or supervisory body of the tenderer *(to be specified if any)*	not applicable
Participant of the group of economic operators representing or leading the group of economic operators *(to be completed if the tender bid is submitted by the group of tenderers)*	not applicable
Name and surname of the person authorised to sign the tender bid	:EO
Contact information of the person authorised to communicate with the Contracting Authority *(name, surname, telephone, e-mail)*	

2. INFORMATION ABOUT EACH PARTNER IN THE GROUP OF TENDERERS

No	Name, legal entity code, address of the partner in the group of tenderers	Collegial management body and/or supervisory body of the partner in the group of tenderers (to be specified if any)	Description of the part of the Contract object to be transferred to the Partner for performance	Value of the part of Services to be provided by the Partner in the tender bid price	
				EUR including VAT	%
1	not applicable				
2	not applicable				
...	not applicable				

3. INFORMATION ON ECONOMIC OPERATORS WHOSE CAPACITIES THE TENDERER RELIES ON TO MEET THE QUALIFICATION REQUIREMENTS SET FORTH BY THE CONTRACTING AUTHORITY (IF ANY)
(to be completed if the tenderer involves other economic operators whose capacities it relies on according to Article 49 of the Law on Public Procurement)

No	Name, code of legal entity of economic operator or name and surname of natural person	Collegial management body and/or supervisory body of the economic operator (to be specified if any)	Reference to the provision in the procurement documents (procurement document and point should be indicated) stipulating the tenderer to rely on the capacity of the economic operator to conform to it	Description of the part of Contract object to be transferred to the economic operator for performance	Value of the part of *Services/Products/Works* to be provided by the Partner in the tender bid price for which economic operators are to be involved	
					EUR including VAT	%
1	not applicable					
2	not applicable					
...	not applicable					

4. INFORMATION ON KNOWN SUB-PROVIDERS AND PART OF THE CONTRACT TRANSFERRED TO THEM FOR PERFORMANCE
(to be completed if the tenderer involves sub-providers)

No	Name of sub-provider, legal entity code, address	Description of the part of the Contract object to be transferred to the sub-provider for performance	Part of the Procurement Contract in the tender bid price transferred to the sub-provider for performance	
			EUR including VAT	%
1	not applicable			
2	not applicable			
...	not applicable			

5. INFORMATION ON THE SPECIALISTS TO BE USED TO PROVE THE TENDERER'S QUALIFICATION AND TO PERFORM THE CONTRACT WHO ARE NOT EMPLOYEES OF THE TENDERER OR THE ECONOMIC OPERATOR(S) INVOLVED BY THE TENDERER AT THE TIME OF SUBMISSION OF THE TENDER BID BUT WHO WOULD BE EMPLOYED IN THE EVENT OF THE CONTRACT AWARD (quasi-sub-providers)

No	Name and surname	Specialist's current place of employment
1	not applicable	
2	not applicable	
...	not applicable	

6. TENDER BID PRICE

6.1. The tender bid price shall be given in euro. If tender bid prices are quoted in foreign currency, they shall be converted into euro according to the euro foreign exchange reference rates published by the European Central Bank. In cases where the European Central Bank does not publish the euro foreign exchange reference rates, according to the euro and foreign exchange reference rate set and published by the Bank of Lithuania on the day of the submission of tender bids.
6.2. When calculating the price, a full scope of the Procurement Object and requirements, price components, etc. specified in the Procurement Documents must be taken into account. After performance of the Contract, the Contracting Authority shall be able to use the Procurement object without additional costs unless explicitly stated otherwise in the Procurement Documents. The VAT is reported separately. If the tenderer is not a VAT payer, it must indicate this in the tender bid, specifying the legal basis. The tenderer must consider whether it is going to become a VAT payer during the performance of the Contract. If the tenderer becomes a VAT payer during the performance of the Contract, it must quote the price including VAT in the tender bid. Tender bid prices including all taxes and VAT shall be evaluated and compared. In case the Contracting Authority has to pay VAT to the state budget for the purchased Procurement Object itself in accordance with the procedure established by the laws governing taxes and the secondary legislation, this tax shall be included in the tender bid price (if the tenderer did not include it in the tender bid, the Contracting Authority shall include it for comparison purposes). The tender bid price must include all taxes and all other direct and indirect costs and fees/charges incurred and/or likely to be incurred by the tenderer in connection with the supply of the **Services**, including but not limited to (except when the Procurement Documents clearly state that certain specific costs are not to be included in the Contract price):
6.2.1. All costs related to the preparation and provision of documents required by the Buyer (if applicable);
6.2.2. Costs of assembling the delivered Products on site and/or start-up of operation and/or maintenance of the Products (if applicable);
6.2.3. Costs of submitting the instructions for use and maintenance provided for in the Technical Specification (if applicable);
6.2.4. Costs for licenses, patents, permits, etc. (if applicable);
6.2.5. Electronic invoicing costs;
6.2.6. Warranty costs of products (if applicable);
6.2.7. (other specified by the contracting authority).
6.3. The total tender bid price/costs including VAT must be indicated with the accuracy of two decimal places. If the third number after the decimal point is from 0 to 4, the second number after the decimal point is left as it is. If the third number after the decimal point is from 5 to 9, the second number after the decimal point is rounded up. E.g., 3.14159 rounded to the hundredth will be 3.14; whereas 3.1153 rounded to the hundredth will be 3.12.

No	Procurement object	Unit of measure	Maximum quantity	Unit rate, in EUR, excluding VAT (to be completed by the tenderer)	Price, in EUR, excluding VAT
1	2	3	4	5	6
1	System installation and configuration	Set	1	2870000,00	2870000,0000
2	Additional development services	Hours	300	100,00	30000,0000
3	System support services	Months	60	18000,00	1080000,0000
				Total maximum comparative tender price, EUR, excluding VAT	**3980000,00**
				VAT*, EUR (tenderer selects the VAT rate) 21	**835800,00**
				Total maximum comparative tender price, EUR, including VAT	**4815800,00**

*If you leave the VAT field empty, indicate the reasons why you do not pay VAT: -_____

NOTES:

1. Total maximum comparative tender bid price in EUR, including VAT, will be used for evaluation of the tender bids. The Initial Contract value will be equal to the tender bid price.
*2. The tender bid price (in Line 1 of the Table) with all included costs, expenses and taxes may not exceed EUR **3 299 532.07, excluding VAT**. The tender bid price (in Line 2 of the Table) with all included costs, expenses and taxes may not exceed **EUR 36 000.00, excluding VAT**. The tender bid price (in Line 3 of the Table) with all included costs, expenses and taxes may not exceed **EUR 3 500 000.00, excluding VAT**. Total bid price may not exceed **EUR 6 835 532.07, excluding VAT**. **Higher price (than in Lines 1-3 of the Table) will be considered by the Contracting Authority to be excessive and unacceptable.***
3. Service fee rates proposed by the tenderer shall be documented and, in case of the Contract award, will be included in the Contract. The tenderer shall be paid for the actually provided Services: quantity of the Services shall be multiplied by the unit rate.
4. The Contracting Authority shall not undertake to purchase total quantity of the Services or any part thereof specified in Line 2 and 3 of the Table above.

7. DOCUMENTS AND INFORMATION ON CONFIDENTIALITY ATTACHED

All documents shall be submitted along with the tender bid using the CVP IS tools unless established otherwise:

No	Documents	Document must be submitted	Entity submitting the document	Does the document contain confidential information? (Yes/no)	Explanation what specific information is confidential in the document and why
1	2	3	4	5	6
1	A copy of the joint venture agreement (if the tender bid is submitted by a group of economic operators)	Along with the tender bid	Tenderers	Select	Not applicable
2	A copy of the power of attorney or other document granting the right to submit and/or sign the tender bid and other documents (if the tender bid is submitted and/or the documents are signed not by the manager of the tenderer, members of the group of economic operators, sub-suppliers/sub-providers or economic operators whose capacity the tenderer relies on)	Along with the tender bid	Tenderers	Select	Not applicable
3	If the tenderer involves economic operators: evidence that these resources will be available throughout the duration of the contractual obligations	Along with the tender bid	Economic operators, sub-supplier	Select	Not applicable
4	The signed ESPD (**Annex 4 to the Procurement Conditions 'ESPD'**). *A separate ESPD shall be completed by: 1) The tenderer; 2) Each member of the group of tenderers (if the tender bid is submitted by a group of tenderers); 3) Each economic operator whose capacity the tenderer relies on pursuant to Article 49 of the Law on Public Procurement (if applicable);	Along with the tender bid	Suppliers, economic operators whose capacity the tenderer relies on	No	
5	Provider's declaration on the absence of the conditions provided for in the Council Regulation (EU) 2022/576 **(Annex 10 to the Procurement Conditions).** In case of doubt as to the correctness of the tenderer's declaration regarding the absence of conditions set out in Council Regulation (EU) 2022/576, the Contracting Authority will ask the tenderer to submit one or several documents proving the data in the declaration as follows: 1. In case a tenderer is a legal entity: 1.1. A copy of instruments of incorporation of the legal entity certified by the manager of the legal entity 1.2. Full extract from the Register of Legal Entities with historical information 1.3. Excerpt from the Information System of Legal Entities Participants 2. In case a tenderer is a natural person: 2.1. Copy of the personal identity document (identity card or passport).	Upon request of the Contracting Authority	Tenderer	No	
6	(Article 37 (9) and Article 47 (9) of the Law on Public Procurement) Declaration of Conformity to National Security Requirements **(Annex 11 to the Procurement Conditions)** in the form established by the Public Procurement Office.	Along with the tender bid	Tenderer	No	
6.1.	When checking the compliance of the tender bid with the requirements of Article 37 (9) and Article 47 (9) of the Law on Public Procurement, the Contracting Authority will ask to submit one or several documents listed below (or relevant documents from a member state or a third country, or other documents acceptable to the Contracting Authority): 1. A copy of instruments of incorporation of the legal entity certified by the manager of the legal entity; 2. Full extract from the Register of Legal Entities with historical information; 3. Excerpt from the Information System of Legal Entities Participants. 4. A copy of the document proving the personal identity (a personal identity card or a passport); 5. A copy of the document certifying the permission to engage in the relevant economic activity (for example, a Business Licence, individual activity certificate, etc.); 6. A certificate on the declared place of residence or a relevant document from a Member State or third country, or any other document acceptable to the Contracting Authority.	Upon request of the Contracting Authority	Potential winner, its sub-suppliers/sub-providers, economic operators whose capacity the potential winner relies on	No	

7.	(Article 45 (2^1) of the Law on Public Procurement Declaration of Conformity **(Annex 7 to the Procurement Conditions).** In case of doubts about the correctness of information provided by the tenderer in the Declaration of Conformity, the Contracting Authority will request the tenderer who submitted the most economically advantageous tender bid to submit the documents (one or several) supporting the information provided in this Declaration and referred to in Article 51(12) of the Law on Public Procurement, or other documents and/or explanations acceptable to the Contracting Authority.	Along with the tender bid	Tenderer	No	
8.	Documents referred to in point 10.1 of **Annex 2 to the Procurement Conditions** 'Technical Specification'	Along with the tender bid	Tenderers	Yes	Point 10.1 refers to the hardware recommendations. The document contains architetural design information of the J4Care solution, which should be kept confidential.
9.	Documents referred to in **Annex 9 to the Procurement Conditions** 'Criteria and Conditions for Evaluation of Tender Bids': a) Tender bid form (Annex 5 to the Procurement Conditions), b) List of specialists and certificate of compliance with qualitative evaluation criteria (Annex 15 to the Procurement Conditions), c) Testimonial from the customer (Annex 16 to the Procurement Conditions).	Along with the tender bid	Tenderers	Yes	The names of the specialists as well as the contract-details of the various customer-agreements are considered confidential.
10	Documents referred to in **Annex 3 to the Procurement Conditions** 'Grounds for Exclusion of Tenderers'. **NOTE**. The requirement is applicable when an international procurement is carried out.	Upon request of the Contracting Authority	Potential winner and economic operators whose capacity the potential winner relies on	No	
11	Documents specified in **Annex 8 to the Procurement Conditions** 'Qualification Requirements for Tenderers and Required Energy Consumption and/or Environmental Protection and/or Social Criteria: a) Certificate prepared according to the template given in Annex 14 to the Procurement Conditions; b) A set of financial statements of the economic operator for the last 3 financial years, and if the economic operator was registered or started its activities later, from the date of registration or start of activities of the economic operator (if this information is available).	Upon request of the Contracting Authority	Potential winner and economic operators whose capacity the potential winner relies on	Yes	The names of the specialists, the contract details of the various customer-agreements as well the financial statements of the company are considered confidential
12	(Article 37 (9) and Article 47 of the Law on Public Procurement) Information about the tenderer **(Annex 13 to the Procurement Conditions)**.	Upon request of the Contracting Authority	Potential winner	Yes	The information about the ownership of the tenderer shall be considered confidential

By signing this tender bid, I hereby declare that:

- I have read the Procurement documents as well as the applicable laws and by-laws of the Republic of Lithuania that govern the procedure of public procurement and may affect any relations between the Contracting Authority and the tenderer arising from this Procurement and/or in relation to this Procurement;
- I agree with the terms, conditions and procedures established in the Procurement Documents;
- The data and information provided in the tender bid documents are correct and include everything necessary for the proper performance of the Contract;
- The tender bid is valid for the term specified in Annex 1 'Time Limits' of the Procurement Conditions, or for the term provided for in the Procurement documents in case of a tender under restricted procedure;
- By signing this tender bid, we confirm that the proposed Procurement Object does not pose a threat to national security;

CEO
(Position of the participant or its authorised person)

(Signature)

(name, surname)

J4CARE GMBH
ENZERSDORFERSTRASSE 7
2340 MÖDLING
AUSTRIA / EUROPE
www.J4CARE.COM

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

1.1. **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.

1.2. **Data Processor** means a natural person or legal entity providing the services referred to in the Special Part.

1.3. **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.

1.4. **JIRA** means a software tool for managing project, product and software development, maintenance tasks and resources.

1.5. **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.

1.6. **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).

1.7. **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.

1.8. **Service Recipient** means the State Enterprise Centre of Registers.

1.9. **Service Provider** means a natural person or legal entity providing the services referred to in the Special Part.

1.10. **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.

1.11. **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.

1.12. **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.

1.13. **Parties** means the Data Controller and the Data Processor jointly.

2. 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.

3. RIGHTS AND OBLIGATIONS OF THE PARTIES

3.1. Data Controller shall:

3.1.1. Be obliged to ensure that the processing of personal data entrusted to the Data Processor has a legal ground;

3.1.2. 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);

3.1.3. 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:

3.1.3.1. Verification must be related only to the processing of personal data under the Arrangement;

3.1.3.2. 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;

3.1.3.3. The additional verification must be carried out in such a way that it does not interfere with the normal activities of the Data Processor;

3.1.3.4. 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.

3.2. Data Processor shall:

3.2.1. 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);

3.2.2. 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;

3.2.3. 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:

3.2.3.1. Pseudonymisation and/or encryption of personal data;

3.2.3.2. Ability to ensure the continuous confidentiality, integrity, accessibility and resilience of data processing systems and services;

3.2.3.3. Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

3.2.3.4. Process for regular testing, inspection and evaluation of technical and organisational measures ensuring the security of processing of personal data;

3.2.4. 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;

3.2.5. 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;

3.2.6. 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:

3.2.6.1. 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;

3.2.6.2. 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;

3.2.7. 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;

3.2.8. 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;

3.2.9. 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;

3.2.10. 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;

3.2.11. 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.

4. RESPONSIBILITY

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

5. FINAL PROVISIONS

5.1. The Arrangement shall come into force on the date of its signing and shall be valid until the expiry of the Service Agreement.

5.2. 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.

2. Data Processor (Service Provider):

J4Care GmbH, commercial register number FN 298641d, with registered office at Enzersdorferstraße 7 2340 Mödling, Austria, phone number e-mail address

3. Service Agreement:

Implementation and configuration of VNA and DICOM based services

4. 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.
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)	-
Conditions for the transfer of data to third countries or international organisations	Will not be transferred

5. Information about sub-processors engaged at the time of signing the Arrangement:

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
-	-	-	-

6. 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 7 to the Special Part of the Service Agreement.

7. Contact details of the Data Controller:

Personal data breach notification	
Requests for the exercise of the data subject's rights under Articles 12-22 of Regulation (EU) 2016/679	
Notification of the authorisation to engage a sub-processor	
Other issues	d

Paslaugų viešojo pirkimo-pardavimo sutarties
specialiosios dalies
Priedas Nr. 6

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

BENDROJI DALIS

1. SĄVOKOS

1.1. **Asmens duomenys** – Specialiojoje dalyje nurodyti asmens duomenys, kuriuos Duomenų valdytojas suteikia teisę tvarkyti Duomenų tvarkytojui Specialiojoje dalyje nustatytu tikslu ir terminu.

1.2. **Duomenų tvarkytojas** – Specialiojoje dalyje nurodytas paslaugas teikiantis fizinis arba juridinis asmuo.

1.3. **Duomenų valdytojas** – valstybės įmonė Registrų centras, veikiantis kaip duomenų valdytojas arba duomenų valdytoją, nurodytą Specialiojoje dalyje, atstovaujantis duomenų tvarkytojas.

1.4. **JIRA** – programinis įrankis, skirtas projekto, produkto bei programinės įrangos kūrimo, priežiūros užduotims ir resursams valdyti.

1.5. **Konfidencialumo pasižadėjimas** – Duomenų valdytojo nustatytos formos pasižadėjimas saugoti valstybės įmonės Registrų centro tvarkomų duomenų paslaptį ir laikytis duomenų saugos reikalavimų, kurį pasirašo Duomenų tvarkytojo įgalioti asmenys, prieš pradedant tvarkyti asmens duomenis.

1.6. **Reglamentas (ES) 2016/679** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

1.7. **Paslaugų teikimo sutartis** – Specialiojoje dalyje nurodyta tarp Paslaugos teikėjo ir Paslaugos gavėjo pasirašyta sutartis dėl paslaugų teikimo, kurios pagrindu yra sudarytas Susitarimas, kaip sudėtinė jos dalis.

1.8. **Paslaugos gavėjas** – valstybės įmonė Registrų centras.

1.9. **Paslaugos teikėjas** – Specialiojoje dalyje nurodytas paslaugas teikiantis fizinis arba juridinis asmuo.

1.10. **Susitarimas** – sudėtinė Paslaugų teikimo sutarties dalis, sudaryta iš Bendrosios ir Specialios dalies, kuriame vadovaujantis Reglamento (ES) 2016/679 28 straipsniu, nustatomos duomenų valdytojo ir duomenų tvarkytojo teisės bei pareigos, duomenų valdytojo vardu tvarkant asmens duomenis.

1.11. **Bendroji dalis** – Susitarimo dalis, kuri nustato bendrąsias asmens duomenų tvarkymo sąlygas, taikomas Susitarimo Šalims.

1.12. **Specialioji dalis** – Susitarimo dalis, kurioje nustatomos konkrečiam Duomenų tvarkytojui taikomos specialios asmens duomenų tvarkymo sąlygos.

1.13. **Šalys** – Duomenų valdytojas ir Duomenų tvarkytojas abu kartu.

2. SUSITARIMO DALYKAS

2.1. Duomenų valdytojas paveda Duomenų tvarkytojui tvarkyti asmens duomenis Susitarime nustatytomis sąlygomis.

3. ŠALIŲ TEISĖS IR PAREIGOS

3.1. Duomenų valdytojas:

3.1.1. privalo užtikrinti, kad asmens duomenų tvarkymas, kurį Duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą;

3.1.2. be Susitarimu nustatytų nurodymų dėl asmens duomenų tvarkymo, turi teisę teikti dokumentais įformintus nurodymus viso asmens duomenų tvarkymo metu. Tokie nurodymai gali būti teikiami raštu Specialiosios dalies 2 punkte nurodytu Duomenų tvarkytojo buveinės adresu, arba elektroniniu paštu, arba registruojami JIRA (kai yra suteiktos prieigos teisės Duomenų tvarkytojo įgaliotiems asmenims);

3.1.3. turi teisę papildomai ir (ar) kitomis nei 3.2.9 papunktyje nurodytomis priemonėmis patikrinti, kaip Duomenų tvarkytojas tvarko asmens duomenis ir (arba) vykdo savo įsipareigojimus pagal šį Susitarimą, toks patikrinimas gali būti atliekamas Šalims susitarus dėl patikrinimo apimties, būdo, kainos ir laiko. Duomenų valdytojas turi teisę papildomam patikrinimui atlikti pasitelkti nepriklausomą auditorių. Bet kuriuo atveju, jeigu Šalys susitaria dėl tokio papildomo patikrinimo, jis turės atitikti šiuos reikalavimus:

3.1.3.1. patikrinimas privalo būti susijęs tik su asmens duomenų tvarkymu pagal Susitarimą;

3.1.3.2. Duomenų valdytojas privalo informuoti Duomenų tvarkytoją apie pageidavimą atlikti papildomą patikrinimą per protingą laiką, kuris privalo būti ne trumpesnis nei 5 darbo dienos;

3.1.3.3. papildomas patikrinimas turi būti atliekamas taip, kad netrukdytų įprastinei Duomenų tvarkytojo veiklai;

3.1.3.4. tuo atveju, jei patikrinimo metu gali būti susipažinta su Duomenų tvarkytojo konfidencialia informacija, Duomenų tvarkytojui pareikalavus, Duomenų valdytojas įsipareigoja saugoti Duomenų tvarkytojo konfidencialią informaciją.

3.2. Duomenų tvarkytojas:

3.2.1. tvarko asmens duomenis pagal Duomenų valdytojo nurodymus, išdėstytus Susitarime, ir kitus raštu (įskaitant elektronine forma) Duomenų valdytojo įformintus nurodymus, išskyrus atvejus, kai duomenis tvarkyti reikalaujama pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurie yra taikomi Duomenų tvarkytojui (tokiais atvejais Duomenų tvarkytojas informuoja Duomenų valdytoją apie šiuos reikalavimus, išskyrus atvejus, kai teisės aktais draudžiama minėtą informaciją pateikti dėl svarbaus viešojo intereso);

3.2.2. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą ir būtų pasirašę Registrų centro pateiktos formos Konfidencialumo pasižadėjimą;

3.2.3. imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį, t. y. techninėmis ir organizacinėmis priemonėmis užtikrina Duomenų valdytojo vardu tvarkomų asmens duomenų saugą, konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais. Saugumo priemonės, kurias privalo įgyvendinti Duomenų tvarkytojas, nurodytos Susitarimo Specialiosios dalies 6 punkte „Nurodymai dėl asmens duomenų tvarkymo saugumo“, o taip pat, priklausomai nuo jų tinkamumo pagal asmens duomenų tvarkymo pobūdį, įskaitant bet neapsiribojant, saugumo priemonės turi būti šios:

3.2.3.1. asmens duomenų pseudonimizavimas ir (ar) šifravimas;

3.2.3.2. galimybė užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

3.2.3.3. galimybė laiku atkurti prieinamumą ir prieigą prie asmens duomenų, įvykus fiziniam ar techniniam incidentui;

3.2.3.4. techninių ir organizacinių priemonių, užtikrinančių duomenų tvarkymo saugumą, reguliaraus testavimo, tikrinimo ir įvertinimo procesas;

3.2.4. užtikrina, kad konkrečiai duomenų tvarkymo veiklai Duomenų valdytojo vardu atlikti pasitelks pagalbinį duomenų tvarkytoją tik turėdamas Specialiojoje dalyje įvardintą Duomenų valdytojo leidimą, o pasitelktam pagalbiniam duomenų tvarkytojui bus nustatytos tos pačios duomenų apsaugos prievolės, nurodytos šiame Susitarime;

3.2.5. atsižvelgdamas į duomenų tvarkymo pobūdį, padeda Duomenų valdytojui taikydamas tinkamas technines ir organizacines priemones, kiek tai įmanoma, kad būtų įvykdyta Duomenų valdytojo prievolė atsakyti į prašymus pasinaudoti Reglamente (ES) 2016/679 nustatytomis duomenų subjekto teisėmis. Jeigu Duomenų tvarkytojas gauna duomenų subjekto prašymą dėl Reglamento (ES) 2016/679 12-22 straipsniuose nustatytų duomenų subjekto teisių įgyvendinimo, privalo šį prašymą nedelsiant, bet ne vėliau kaip per 3 darbo dienas persiųsti Duomenų valdytojui elektroniniu paštu nurodytu Specialiosios dalies 7 punkte;

3.2.6. padeda Duomenų valdytojui užtikrinti Reglamento (ES) 2016/679 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į duomenų tvarkymo pobūdį ir turimą informaciją:

3.2.6.1. ne vėliau kaip per 24 valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo momento raštu Specialiosios dalies 7 punkte nurodytais adresais, informuoja Duomenų valdytoją apie įvykusį tvarkomų asmens duomenų saugumo pažeidimą ir pateikia pranešimą, jame nurodydamas Reglamento (ES) 2016/679 33 straipsnio 3 dalyje išvardytą informaciją bei imasi priemonių pažeidimui nedelsiant sustabdyti ir užkertančių kelią tolesnei žalai dėl įvykusio asmens duomenų saugumo pažeidimo bei mažinančių įvykusio asmens duomenų saugumo pažeidimo padarinius. Jeigu visos informacijos neįmanoma pateikti tuo pačiu metu, informacija toliau nedelsiant turi būti teikiama etapais. Duomenų valdytojo prašymu per nurodytą laikotarpį Duomenų tvarkytojas pateikia papildomą informaciją, reikalingą Duomenų valdytojui vertinant asmens duomenų saugumo pažeidimo aplinkybes, įskaitant, bet neapsiribojant, Duomenų tvarkytojo asmens duomenų saugumo pažeidimų žurnalo išrašą;

3.2.6.2. gavęs Duomenų valdytojo prašymą, per Duomenų valdytojo nurodytą terminą pateikia informaciją, kuri Duomenų valdytojui būtina atliekant poveikio duomenų apsaugai vertinimą, vadovaujantis Reglamento (ES) 2016/679 35 straipsniu, įskaitant informacijos pateikimą, kai Duomenų valdytojas priima sprendimą kreiptis į Valstybinę duomenų apsaugos inspekciją dėl išankstinių konsultacijų;

3.2.7. užbaigęs teikti su duomenų tvarkymu susijusias paslaugas, atsižvelgdamas į asmens Duomenų valdytojo nurodymus, pateiktus Specialiojoje dalyje, ištrina arba grąžina Duomenų valdytojui visus asmens duomenis ir ištrina esamas jų kopijas, išskyrus atvejus, kai Europos Sąjungos ar Lietuvos Respublikos teisės aktai nustato Duomenų tvarkytojo pareigą asmens duomenis saugoti. Jei Duomenų tvarkytojui taikoma prievolė pagal teisės aktus saugoti asmens duomenis, Duomenų tvarkytojas, prieš pradėdamas tvarkyti asmens duomenis Duomenų valdytojo vardu, Specialiojoje dalyje privalo nurodyti jam taikomus teisės aktus, kuriais jis yra įpareigotas saugoti asmens duomenis;

3.2.8. įsipareigoja nekopijuoti, neperkelti, nesaugoti ir kitaip netvarkyti asmens duomenų Duomenų tvarkytojo IT infrastruktūroje, kai pagal Duomenų valdytojo Specialiojoje dalyje pateiktus nurodymus nustatyta, kad asmens duomenys tvarkomi tik Duomenų valdytojo IT infrastruktūroje;

3.2.9. įsipareigoja periodiškai savo iniciatyva ir sąskaita tikrinti, ar atitinkamos techninės ir organizacinės priemonės atitinka duomenų tvarkymo pobūdį, apimtį, kontekstą ir tikslus, o taip pat riziką, susijusią su duomenų tvarkymu, fizinių asmenų teisių ir laisvių atžvilgiu. Duomenų tvarkytojas šį tikrinimą gali atlikti pats arba pasitelkti nepriklausomą auditorių. Duomenų valdytojo rašytiniu

prašymu tikrinimo ataskaitą arba jos ištrauką, Duomenų tvarkytojas privalo pateikti Duomenų valdytojui;

3.2.10. jei Duomenų valdytojas nenurodo Susitarime arba vėliau nepateikia dokumentais pagrįstų nurodymų dėl asmens duomenų perdavimo į trečiąją valstybę ar tarptautinėms organizacijoms, Duomenų tvarkytojas neturi teisės atlikti tokį perdavimą pagal šį Susitarimą, išskyrus, jei asmens duomenis trečiosioms valstybėms ar tarptautinėms organizacijoms reikia perduoti pagal Europos Sąjungos ar jos valstybės narės teisės aktus, kurių turi laikytis Duomenų tvarkytojas, nors Duomenų valdytojas nedavė nurodymų Duomenų tvarkytojui tai atlikti. Tokiu atveju, apie šį teisinį reikalavimą Duomenų tvarkytojas informuoja Duomenų valdytoją, Specialiojoje dalyje nurodydamas jam taikomus teisės aktus, kuriais jis yra įpareigotas perduoti asmens duomenis į trečiąją valstybę ar tarptautinėms organizacijoms, nebent tas teisės aktas draudžia perduoti tokią informaciją;

3.2.11. turėdamas pagrįstų įrodymų, kad Duomenų valdytojo nurodymu gali būti pažeidžiami teisės aktai, turi teisę sustabdyti tokio nurodymo vykdymą prieš tai raštu Specialiosios dalies 7 punkte nurodytais adresais informavęs Duomenų valdytoją. Duomenų valdytojui įrodžius nurodymo atitiktį teisės aktams arba iš dalies jį pakeitus, nurodymas turi būti vykdomas.

4. ATSAKOMYBĖ

4.1. Duomenų valdytojas yra atsakingas už tai, kad jo duodami nurodymai Duomenų tvarkytojui dėl asmens duomenų tvarkymo atitiktų Reglamento (ES) 2016/679 reikalavimus.

4.2. Duomenų tvarkytojas yra atsakingas už tai, kad tvarkytų Duomenų valdytojo pateiktus asmens duomenis, laikydamasis šio Susitarimo ir Duomenų valdytojo nurodymų.

4.3. Jei pasitelktas kitas duomenų tvarkytojas nevykdo arba netinkamai vykdo asmens duomenų apsaugos prievoles, Duomenų tvarkytojas išlieka visiškai atsakingas Duomenų valdytojui už pasitelkto kito duomenų tvarkytojo prievolių vykdymą.

4.4. Susitarimo sąlygos neatleidžia Šalių nuo kitų pareigų, kurios joms taikomos pagal Reglamentą (ES) 2016/679 ar kitus teisės aktus.

5. BAIGIAMOSIOS NUOSTATOS

5.1. Susitarimas įsigalioja nuo jo pasirašymo dienos ir galioja iki Paslaugų teikimo sutarties galiojimo dienos.

5.2. Bet kokie nesutarimai ar ginčai, kylantys tarp Šalių dėl Susitarimo, sprendžiami derybų būdu, o jeigu tokiu būdu ginčų išspręsti nepavyksta, jie sprendžiami Lietuvos Respublikos teisme pagal Duomenų valdytojo registruotos buveinės vietą, vadovaujantis Lietuvos Respublikoje galiojančiais įstatymais ar kitais teisės aktais.

SUSITARIMAS DĖL ASMENS DUOMENŲ TVARKYMO

SPECIALIOJI DALIS

1. Duomenų valdytojas (Paslaugos gavėjas):

Valstybės įmonė Registrų centras, juridinio asmens kodas 124110246, kurios registruota buveinė yra Studentų g. 39, Vilnius, telefono ryšio numeris +370 5 268 8262, elektroninio pašto adresas info@registrucentras.lt, veikiantis duomenų valdytojo Lietuvos Respublikos sveikatos apsaugos ministerijos, juridinio asmens kodas 188603472, kurios registruota buveinė Vilniaus g. 33, Vilnius, telefono ryšio numeris +370 5 268 5110, elektroninio pašto adresas ministerija@sam.lt vardu.

2. Duomenų tvarkytojas (Paslaugos teikėjas):

J4Care GmbH, juridinio asmens kodas FN 298641d, kurio registruota buveinė Enzersdorferstraße 7 2340 Mödling, Austria, telefono numeris , elektroninio pašto adresas j

3. Paslaugų teikimo sutartis:

DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas.

4. Nuostatos apie asmens duomenų tvarkymą:

Asmens duomenų tvarkymo tikslas	I pirkimo objekto dalis – DICOM standartu paremtų servisų ir VNA diegimas bei konfigūravimas.
Asmens duomenų tvarkymo pobūdis ir duomenų tvarkymo operacijos	Susipažinti su esamu ESPBI IS sprendimu, jo funkcijomis (galimybė matyti asmens duomenis ESPBI IS testinėje aplinkoje); Atlikti sukurtos Sistemos bandomąją eksploataciją; Atlikti sukurtos Sistemos diegimą ir testavimą; Duomenų perkėlimas ir migravimas į naujai sukurtą posistemę; Vykdyti garantinę priežiūrą (su galimybe matyti asmens duomenis ESPBI IS produkcinėje aplinkoje).
Asmens duomenų subjektų kategorijos	ESPBI IS naudotojai – pacientai arba jų atstovai, sveikatos priežiūros specialistai, testavime dalyvaujantys asmenys.
Tvarkomų asmens duomenų rūšys	ESPBI IS naudotojų duomenys nurodyti Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarime Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo“ (toliau-Nuostatai) III skyriuje. Testavime dalyvaujančių asmenų (Vardas, Pavardė, Asmens kodas, pareigos, kontaktinė informacija).
Asmens duomenų tvarkymo vieta	Duomenų valdytojo IT infrastruktūroje, adresu Studentų g. 39, Vilnius.
Asmens duomenų tvarkymo trukmė	Paslaugų teikimo sutarties galiojimo laikotarpis.

Leidimas pasitelkti kitą duomenų tvarkytoją, kuris bus pasitelkiamas po Susitarimo pasirašymo	Duomenų tvarkytojas gali pasitelkti kitą duomenų tvarkytoją tik turėdamas išankstinį konkretų Duomenų valdytojo leidimą. Apie planuojamą pasitelkti kitą duomenų tvarkytoją Duomenų tvarkytojas informuoja Duomenų valdytoją oficialiu raštu Specialiosios dalies 7 punkte nurodytu adresu, ne vėliau kaip prieš 20 darbo dienų iki planuojamo pasitelkimo, o Duomenų valdytojas per 10 darbo dienų raštu Specialiosios dalies 2 punkte nurodytais kontaktais (raštas siunčiamas paštu arba elektroniniu paštu) pateikia Duomenų tvarkytojui leidimą arba nesutikimą.
Duomenų valdytojo nurodymai dėl asmens duomenų ištrynimo arba grąžinimo, pabaigus tvarkyti duomenis	Nutraukus paslaugų teikimą Duomenų tvarkytojui, kuris tvarkė asmens duomenis Duomenų valdytojo infrastruktūroje, nedelsiant (tą pačią dieną) panaikinama prieiga prie Duomenų valdytojo informacinių išteklių.
Duomenų tvarkytojo pareiškimai, pagrindžiami Europos Sąjungos ir (ar) Lietuvos Respublikos teisės aktais, dėl privalomo asmens duomenų saugojimo (jei toks taikomas Duomenų tvarkytojui)	-
Duomenų perdavimo į trečiąsias valstybes arba tarptautinėms organizacijoms sąlygos	Nebus perduodama

5. Informacija apie Susitarimo pasirašymo momentu pasitelktus kitus asmens duomenų tvarkytojus:

Pavadinimas, vardas, pavardė	Įmonės kodas / gimimo data arba individualios veiklos numeris	Buveinės adresas / gyvenamosios vietos adresas	Duomenų tvarkymo aprašymas
-	-	-	-

6. Nurodymai dėl asmens duomenų tvarkymo saugumo:

Duomenų tvarkymo saugumo priemonės	Duomenų tvarkytojas privalo laikytis Susitarimo dėl taikomų organizacinių ir techninių kibernetinio saugumo reikalavimų, kurie yra pateikti atskirame Paslaugų teikimo sutarties specialiosios dalies priede Nr. 7.

7. Duomenų valdytojo kontaktai:

Pranešimas apie asmens duomenų saugumo pažeidimą	d
Prašymai dėl Reglamento (ES) 2016/679 12-22 straipsniuose nustatytų duomenų subjekto teisių įgyvendinimo	duomenusauga@registrucentras.lt
Pranešimas dėl leidimo pasitelkti pagalbinį duomenų tvarkytoją	
Kiti klausimai	d

Annex No. 7
To the Special Part of the Contract for the
Public Procurement-Sale of Services

ARRANGEMENT ON APPLICABLE ORGANISATIONAL AND TECHNICAL CYBER SECURITY REQUIREMENTS

When performing the Contract for the Public Procurement-Sale of Services (hereinafter referred to as the Contract), the Supplier/Provider shall be obliged to ensure an adequate level of data security, i.e. the constant confidentiality, integrity, availability of the personal data processed and resilience of the data processing IT systems, and to make appropriate decisions on the use of technical and organisational security measures for this purpose. If the Supplier/Provider serves a critical information and communication technology (hereinafter referred to as the ICT) infrastructure, or provides other essential services in Lithuania provided for in Annex 1 to the Law on Cyber Security of the Republic of Lithuania, it shall comply with the provisions of the Cyber Security Requirements approved by Resolution No 818 of the Government of the Republic of Lithuania of 13 August 2018 On the Implementation of the Law on Cyber Security of the Republic of Lithuania applicable to the central cyber security entity. In the case of a foreign Supplier/Provider who processes the data transferred to it outside the ICT infrastructure of the State Enterprise Centre of Registers (hereinafter referred to as the Centre of Registers), the requirements of international standards such as ISO/IEC 27001 or equivalent standards (NIST CSF, SOC 2, etc.) shall be complied with.

The Supplier/Provider undertakes to ensure the implementation of the following organisational and technical cyber security requirements:

1. Organisational security measures for data processing	1.1.	Upon conclusion of the Contract, the employees appointed by the Supplier/Provider who will provide services under this Contract and connect to the ICT infrastructure of the Centre of Registers shall be required to read through the Cyber Security Policy adopted by the Information Resource Manager and the implementing legislation, and to comply with the established requirements. In cases where the Supplier/Provider is transferred to process the data of the Centre of Registers in its (Supplier's/Provider's) infrastructure, the Supplier/Provider must comply with the information and/or cyber security policy adopted by the Supplier's/Provider's organisation.
	1.2.	Maintain the confidentiality of information transmitted, stored or otherwise processed throughout the term of the Contract and thereafter, and to undertake in writing to protect such information prior to the commencement of such processing.
	1.3.	Ensure the security of the login data received and not to disclose it to third parties.
	1.4.	Grant, modify and/or revoke user rights on a need-to-know principle, or ensure that access to information is limited to execution of specific functions (carrying out work) and/or for a specific period.
	1.5.	The Supplier/Provider shall apply appropriate and adequate procedures for granting of rights or lifting of obligations, transfer or assignment of roles and responsibilities in the event of dismissal and change of their functions within its organisation.

	1.6.	The Supplier/Provider must ensure that suppliers/providers (sub-suppliers/sub-providers) involved comply with the same information and cyber security requirements.
	1.7.	The Supplier/Provider shall immediately inform the Centre of Registers of the termination of employment relationship with the employee of the organisation who has been granted access to the information processed in the ICT infrastructure of the Centre of Registers.
	1.8.	The Supplier/Provider shall have the obligation to immediately inform about any major and/or other electronic information security incidents observed in the information technology infrastructure of the Centre of Registers during the performance of the Contract, non-functioning or improperly functioning security measures, non-compliance with information security requirements, signs of criminal activity, detected security gaps (vulnerabilities) that pose a risk to the networks and information systems of the cyber security entity and other important safety events. It shall also inform the Centre of Registers, but not later than within 24 hours, when the said cases have been identified in the information systems infrastructure managed by the Supplier/Provider, which affect the data processed by the Centre of Registers. It shall provide the cyber security entity with a report on the investigation of a cyber incident when the investigation is completed.
	1.9.	The Supplier/Provider shall be responsible for facilitating a cyber security entity or its authorised service providers to carry out a Supplier's/Provider's compliance audit (including an unplanned one) during the Contract period or in the event of a major incident.
	1.10.	Perform the Service level Agreement, SLA.
	1.11.	Use only legal software.
2. Technical security measures for data processing	2.1.	An access control system shall be in place and implemented, which is applicable to all users of the IT system. The access control system must allow the creation, validation, review and deletion of user accounts.
	2.2.	The use of shared user accounts shall be avoided. Where a shared user account is necessary, all users of the shared account shall have the same rights and obligations.
	2.3.	An authentication mechanism must be in place allowing access to the IT system. The minimum requirement for the user to log in to the IT system shall be a username and a password. The password shall be created according to a certain level of complexity. The password must consist of letters, numbers and special characters; the personal information (such as date of birth, family names, etc.) must not be used for passwords. The user password must consist of at least 10 characters, which must be changed at least every six months; and the

	administrator password must consist of at least 15 characters, which must be changed at least every six months. The security of the login data must be ensured. All measures must be taken to prevent login names and passwords becoming known to third parties. 2.4. The password must be prohibited from being stored in the computer workstation or its software. 2.5. The access control system must be able to detect and prevent the use of passwords that do not meet a certain level of complexity. 2.6. Technical logs must be implemented for each IT system, which is used to process personal data under the Contract. Technical logs shall contain all possible information on access to personal data (e.g. date, time, review, modification, cancellation). The retention period shall be at least 6 months. Technical logs shall bear time stamps and shall be protected against possible tampering, falsification or unauthorized access. Time-keeping mechanisms used in IT systems shall be synchronised according to the common time reference source. 2.7. Protection of computer workstations used for data processing under the Arrangement: 2.7.1. Users of workplaces may not be able to disable or bypass and avoid IT system security settings. 2.7.2. Users may not have privileges (rights) to install, remove, administer unauthorised software. 2.7.3. After work is completed, or when leaving the workplace, the network and information systems must be disconnected, the screen saver with a password must be activated. 2.7.4. Critical security updates for the operating system of computer workstations must be installed regularly and immediately. 2.7.5. Anti-virus applications and their databases of information about viruses and malware must be updated at least once a day. 2.7.6. Where access to the IT systems used for processing data under the Arrangement is provided via the Internet, data must be encrypted using Virtual Private Network (VPN) technology with TLS/SSL certificate or using Access Point Name (APN) technology and applying streaming data encryption with TLS/SSL certificate when VPN technology is not supported by mobile devices. 2.7.7. Wireless connection to IT systems must be allowed only for certain users and processes. The wireless subnet shall be separated from other subnets. Wireless communication must be encrypted in accordance with the encryption length key recommended by good security practices. One should use keys and protocol versions, which are generally acknowledged as secure. The standard manufacturer keys must be changed in the wireless access point.

	2.7.8. Mobile and portable devices to be used for work with information systems must be registered and authorised before their use. 2.7.9. Mobile, portable devices must have a sufficient level of access control procedures, as well as other equipment used to process personal data. 2.8. The confidentiality of sensitive information transmitted to a cyber security entity through public electronic communications networks must be ensured through encryption and must be protected by passwords. 2.9. Network and information system data stored on mobile devices and external computer media must be encrypted. One should encrypt data at the hard disk level. 2.10. Before removing any data medium, all data contained therein must be destroyed using a dedicated software that supports reliable data destruction algorithms. If this is not possible (e.g. in case of USB, DVD media), the data media must be destroyed physically without the possibility of restoring it, e.g. using shredders or other mechanical means. 2.11. Physical protection of the environment and premises with IT system infrastructure from unauthorised access must be implemented.

-Pasirinkti- viešojo pirkimo-pardavimo
sutarties specialiosios dalies
Priedas Nr. 7

SUSITARIMAS DĖL TAIKOMŲ ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ

Vykdydamas -Pasirinkti- viešojo pirkimo–pardavimo sutartį (toliau – Sutartis) Tiekėjas privalo užtikrinti tinkamą duomenų saugumo lygį, t. y. nuolatinį tvarkomų asmens duomenų konfidencialumą, vientisumą, prieinamumą ir duomenų tvarkymo IT sistemų atsparumą, ir šiuo tikslu priimti tinkamus sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo. Jei Tiekėjas aptarnauja kritinę informacinių ir ryšių technologijų (toliau – IRT) infrastruktūrą arba teikia kitas esmines Lietuvos Respublikos kibernetinio saugumo įstatymo 1 priede numatytas paslaugas Lietuvoje, jis laikosi Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo", reikalavimų, taikomų kibernetinio saugumo esminiam subjektui. Jeigu tai užsienio Tiekėjas, kuris jam perduotus duomenis tvarko ne valstybės įmonės Registrų centro (toliau – Registrų centro) IRT infrastruktūroje, turi būti laikomasi tarptautinių standartų kaip ISO/IEC 27001 reikalavimų arba lygiaverčių standartų (NIST CSF, SOC 2 ir pan.).

Tiekėjas įsipareigoja užtikrinti toliau išvardintų organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą:

1. Organizacinės duomenų tvarkymo saugumo priemonės	1.1. Sudarius Sutartį, Tiekėjo paskirti darbuotojai, kurie teiks paslaugas pagal šią Sutartį ir jungsis prie Registrų centro IRT infrastruktūros, privalo susipažinti su informacinio ištekliaus valdytojo patvirtinta Kibernetinio saugumo politika ir ją įgyvendinančiais teisės aktais bei laikytis nustatytų reikalavimų. Tais atvejais, kai Tiekėjui yra perduodama tvarkyti Registrų centro duomenis savo (Tiekėjo) infrastruktūroje, Tiekėjui būtina vadovautis Tiekėjo organizacijoje patvirtinta informacijos ir (ar) kibernetinio saugumo politika. 1.2. Visą Sutarties galiojimo laikotarpį ir po jo užtikrinti perduodamos, saugomos ar kitais būdais tvarkomos informacijos konfidencialumą, o iki pradedant tokią informaciją tvarkyti, raštiškai įsipareigoti saugoti tokio pobūdžio informaciją. 1.3. Užtikrinti gautų prisijungimo duomenų saugumą ir neatskleisti jų trečiosioms šalims. 1.4. Naudotojų teises suteikti, keisti ir (ar) panaikinti laikantis principo „Būtina žinoti" arba užtikrinti, kad teisė prieiti prie informacijos būtų suteikta tik konkrečioms funkcijoms įvykdyti (darbui atlikti) ir (ar) konkrečiai apibrėžtam laikotarpiui. 1.5. Tiekėjas turi taikyti atitinkamas ir adekvačias teisių suteikimo ar pareigų atšaukimo, vaidmenų ir atsakomybių perdavimo ar perleidimo darbuotojo atleidimo bei jų funkcijų pasikeitimo atveju procedūras savo organizacijoje. 1.6. Tiekėjas turi užtikrinti, kad jo pasitelkti tiekėjai (subtiekėjai) atitiktų tuos pačius informacijos ir kibernetinio saugumo reikalavimus.

	1.7.	Tiekėjas turi nedelsiant informuoti Registrų centrą apie nutrūkusius darbo santykius su organizacijos darbuotoju, kuriam buvo suteikta prieiga prie Registrų centro IRT infrastruktūroje tvarkomos informacijos.
	1.8.	Tiekėjo pareiga nedelsiant informuoti apie Sutarties vykdymo metu Registrų centro informacinių technologijų infrastruktūroje pastebėtus didelius ir (ar) kitus elektroninės informacijos saugos incidentus, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, informacijos saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, aptiktas saugumo spragas (pažeidžiamumai), kurie kelia riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms bei kitus svarbius saugai įvykius. Taip pat informuoti Registrų centrą, bet ne vėliau kaip per 24 val., kai Tiekėjo valdomoje informacinių sistemų infrastruktūroje buvo nustatyti minėti atvejai, kurie įtakoja Registrų centro tvarkomus duomenis. Kibernetinio saugumo subjektui pateikti kibernetinio incidento tyrimo ataskaitą, kai bus užbaigtas tyrimas.
	1.9.	Tiekėjo pareiga sudaryti sąlygas Kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties auditą (įskaitant neplaninį) sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui.
	1.10.	Vykdyti sutartinius paslaugų teikimo įsipareigojimus (angl. *Service Level Agreement*, SLA).
	1.11.	Naudoti tik legalią programinę įrangą.
2. Techninės duomenų tvarkymo saugumo priemonės	2.1.	Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.
	2.2.	Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.
	2.3.	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių, slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai). Naudotojo slaptažodį turi sudaryti ne mažiau kaip 10 simbolių, kuris turi būti keičiamas ne rečiau kaip kas šeši mėnesiai, o administratoriaus slaptažodį turi sudaryti ne mažiau kaip 15 simbolių, kuris turi būti keičiamas ne rečiau kaip kas šeši mėnesiai. Turi būti užtikrintas prisijungimo duomenų saugumas.

	Turi būti imtasi visų priemonių, kad prisijungimo vardai ir slaptažodžiai netaptų žinomi tretiesiems asmenims. 2.4. Kompiuterinėje darbo vietoje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį. 2.5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. 2.6. Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti pagal Susitarimą. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Saugojimo terminas – ne trumpiau kaip 6 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. 2.7. Kompiuterinių darbo vietų, naudojamų duomenų tvarkymui pagal Susitarimą, apsauga: 2.7.1. darbo vietų naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų; 2.7.2. naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos; 2.7.3. baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu. 2.7.4. kritiniai kompiuterinių darbo vietų operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant; 2.7.5. antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą; 2.7.6. kai prieiga prie naudojamų IT sistemų, susijusių su duomenų tvarkymu pagal Susitarimą, yra vykdoma internetu, duomenys turi būti šifruojami taikant virtualaus privataus tinklo (VPN) technologiją su TLS / SSL sertifikatu arba naudojama privataus prieigos taško (angl. *Access Point Name*, APN) per mobiliojo ryšio operatorių technologija, taikant perduodamų duomenų šifravimą sraute su TLS / SSL sertifikatu, kai VPN technologija nėra palaikoma mobiliųjų įrenginių. 2.7.7. belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu. Naudoti visuotinai saugiais pripažįstamus raktus ir protokolų versijas. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai.

	2.7.8. mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti; 2.7.9. mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti; 2.8. Viešaisiais elektroninių ryšių tinklais perduodamos kibernetinio saugumo subjektui jautrios informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą bei turi būti apsaugota slaptažodžiais. 2.9. Mobiliųjų įrenginių laikmenose ir išorinėse kompiuterinėse laikmenose laikomi tinklų ir informacinių sistemų duomenys turi būti šifruojami. Šifruoti duomenis kietojo disko lygmenyje. 2.10. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., USB, DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti, pvz. naudojant tam skirtus smulkintuvus arba kitas mechanines priemones. 2.11. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas	Valstybės įmonė Registrų centras
Dokumento pavadinimas (antraštė)	DICOM standartu paremtų servisų ir VNA diegimo bei konfigūravimo paslaugų pirkimo pardavimo sutartis (Pirkimas: Kompleksinio MedVAIS modernizavimo sprendimo sukūrimas ir įdiegimas, pirkimo CVP IS ID 2254548)
Dokumento registracijos data ir numeris	2025-09-10 Nr. ST-262 (5.7 Mr)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	PDF-LT-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Parašo sukūrimo data ir laikas	2025-05-27 18:21
Parašo formatas	PAdES-T
Laiko žymoje nurodytas laikas	2025-09-11 01:00
Informacija apie sertifikavimo paslaugų teikėją	a-sign-premium-mobile-05
Sertifikato galiojimo laikas	2023-07-05 13:07 - 2028-07-05 13:07
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	s Generalinis direktorius
Parašo sukūrimo data ir laikas	2025-09-09 16:28
Parašo formatas	PAdES-T
Laiko žymoje nurodytas laikas	2025-09-09 16:28
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA-2
Sertifikato galiojimo laikas	2023-11-17 10:44 - 2028-11-15 10:44
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	J
Parašo sukūrimo data ir laikas	2025-09-10 02:27
Parašo formatas	PAdES-T
Laiko žymoje nurodytas laikas	2025-09-11 01:00
Informacija apie sertifikavimo paslaugų teikėją	a-sign-premium-mobile-05
Sertifikato galiojimo laikas	2023-07-05 13:07 - 2028-07-05 13:07
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Parašo sukūrimo data ir laikas	2025-09-10 15:51
Parašo formatas	PAdES-T
Laiko žymoje nurodytas laikas	2025-09-10 15:51

Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA-2
Sertifikato galiojimo laikas	2025-02-21 14:55 - 2027-02-21 14:55
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Sisteminis parašas
Parašo sukūrimo data ir laikas	2025-09-11 01:00
Parašo formatas	PAdES-LTV
Laiko žymoje nurodytas laikas	2025-09-11 01:00
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA-2
Sertifikato galiojimo laikas	2024-02-08 13:49 - 2030-05-20 15:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20250822.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Rinkmenos antraštės eilutėje nurodyta ne „1.7“ versija. Dokumento versija „%PDF-1.4“ Dokumento turinys buvo pakeistas po pasirašymo PDF parašo "Signature70186ad5-b47d-4157-bb69-841e8145789c" žodyno „Contents“ lauke saugomų PDF elektroninio parašo duomenų struktūroje (CAdES) yra klaidų (2) PDF parašo "Signature4ed4beac-45e9-44cb-b154-3d0bf4d08299" žodyno „Contents“ lauke saugomų PDF elektroninio parašo duomenų struktūroje (CAdES) yra klaidų (2)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	
Paieškos nuoroda	-
Papildomi metaduomenys	-