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

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.

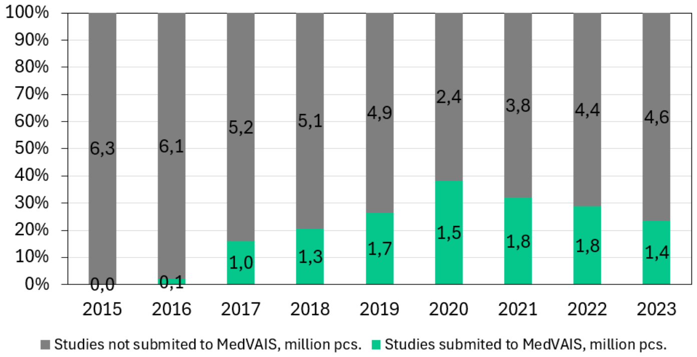

Figure 1. Number of medical images in MedVAIS and Lithuania through 2015 – 2023.

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.

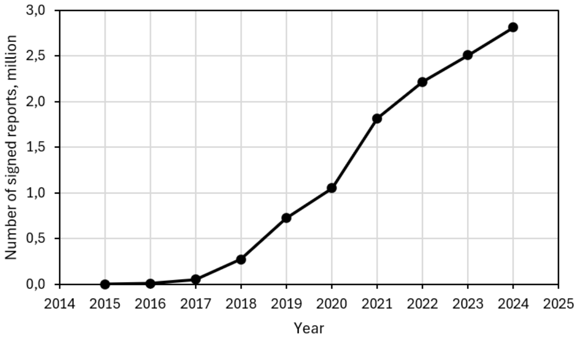

Figure 2. Signed reports submitted to MedVAIS through 2015 – 2024.

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.

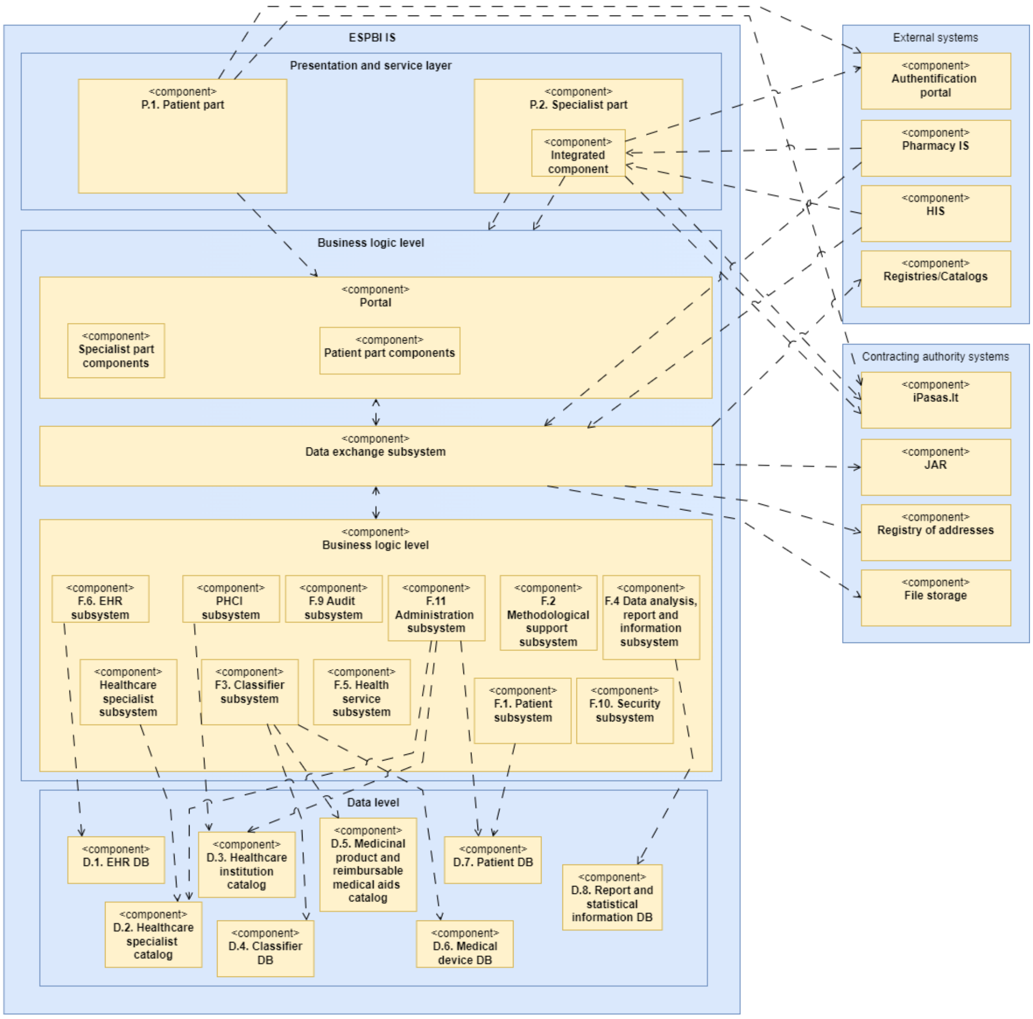
ESPBI IS
Presentation and service layer
<component> P.1. Patient part
<component> P.2. Specialist part
<component> Integrated component
Business logic level
<component> Portal
<component> Specialist part components
<component> Patient part components
<component> Data exchange subsystem
<component> Business logic level
<component> F.6. EHR subsystem
<component> PHCI subsystem
<component> F.9 Audit subsystem
<component> F.11 Administration subsystem
<component> F.2 Methodological support subsystem
<component> F.4 Data analysis, report and information subsystem
<component> Healthcare specialist subsystem
<component> F3. Classifier subsystem
<component> F.5. Health service subsystem
<component> F.1. Patient subsystem
<component> F.10. Security subsystem
Data level
<component> D.1. EHR DB
<component> D.3. Healthcare institution catalog
<component> D.5. Medicinal product and reimbursable medical aids catalog
<component> D.7. Patient DB
<component> D.8. Report and statistical information DB
<component> D.2. Healthcare specialist catalog
<component> D.4. Classifier DB
<component> D.6. Medical device DB
External systems
<component> Authentification portal
<component> Pharmacy IS
<component> HIS
<component> Registries/Catalogs
Contracting authority systems
<component> iPasas.lt
<component> JAR
<component> Registry of addresses
<component> File storage

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.

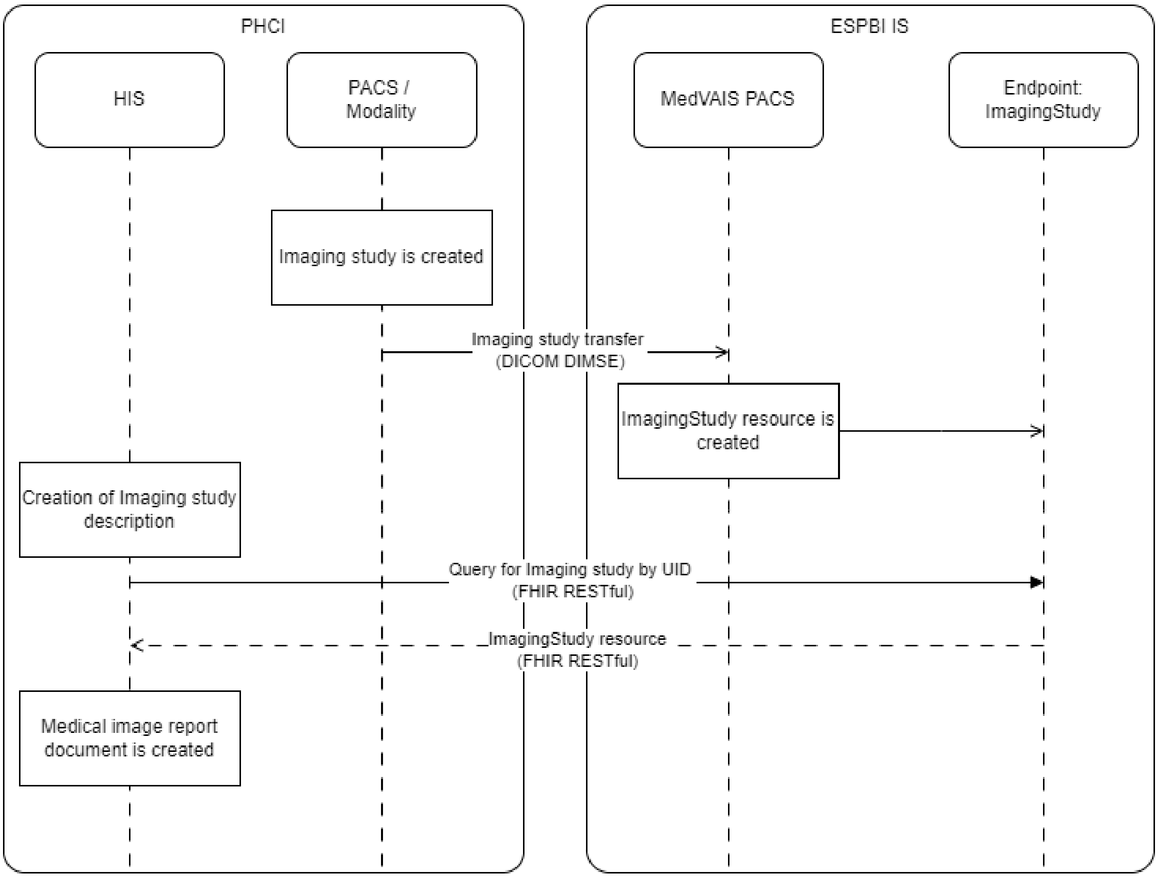
PHCI
ESPBI IS
HIS
PACS / Modality
MedVAIS PACS
Endpoint: ImagingStudy
Imaging study is created
Imaging study transfer (DICOM DIMSE)
ImagingStudy resource is created
Creation of Imaging study description
Query for Imaging study by UID (FHIR RESTful)
ImagingStudy resource (FHIR RESTful)
Medical image report document is created

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.

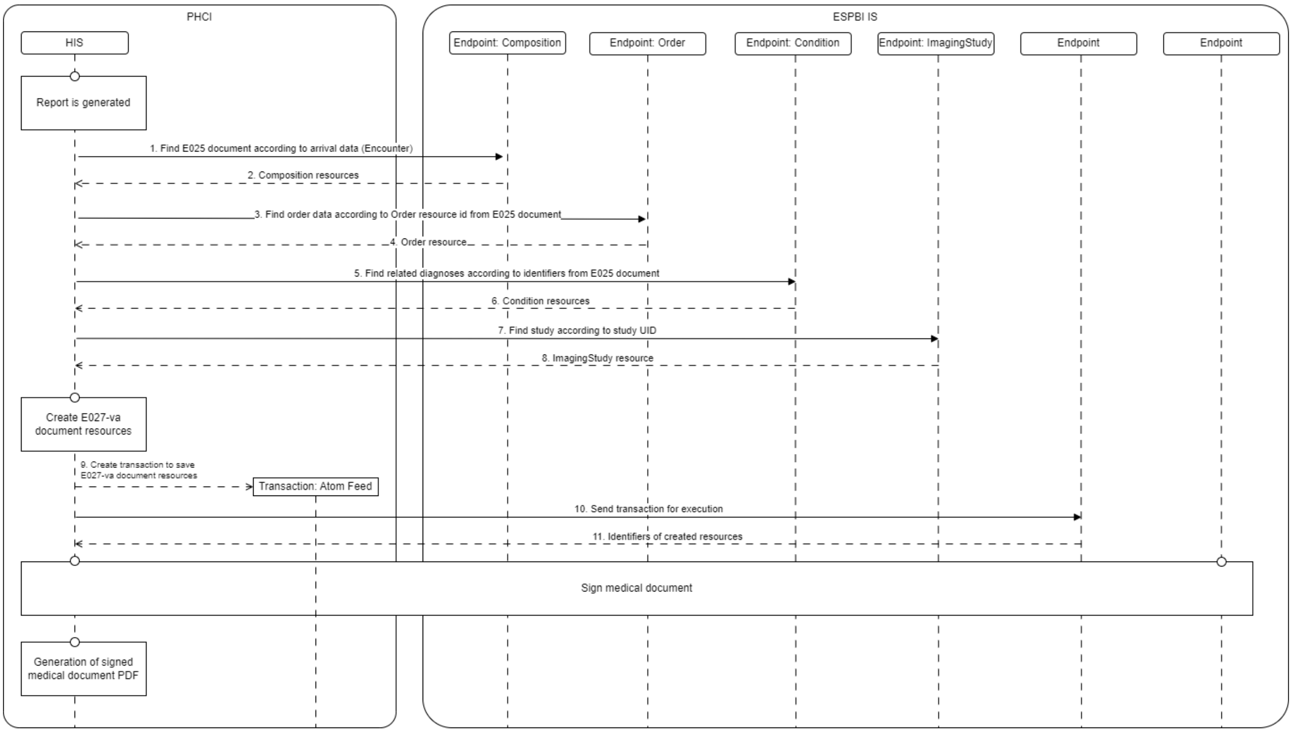
PHCI
ESPBI IS
HIS
Endpoint: Composition
Endpoint: Order
Endpoint: Condition
Endpoint: ImagingStudy
Endpoint
Endpoint
Report is generated
1. Find E025 document according to arrival data (Encounter)
2. Composition resources
3. Find order data according to Order resource id from E025 document
4. Order resource
5. Find related diagnoses according to identifiers from E025 document
6. Condition resources
7. Find study according to study UID
8. ImagingStudy resource
Create E027-va document resources
9. Create transaction to save E027-va document resources
Transaction: Atom Feed
10. Send transaction for execution
11. Identifiers of created resources
Sign medical document
Generation of signed medical document PDF

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.

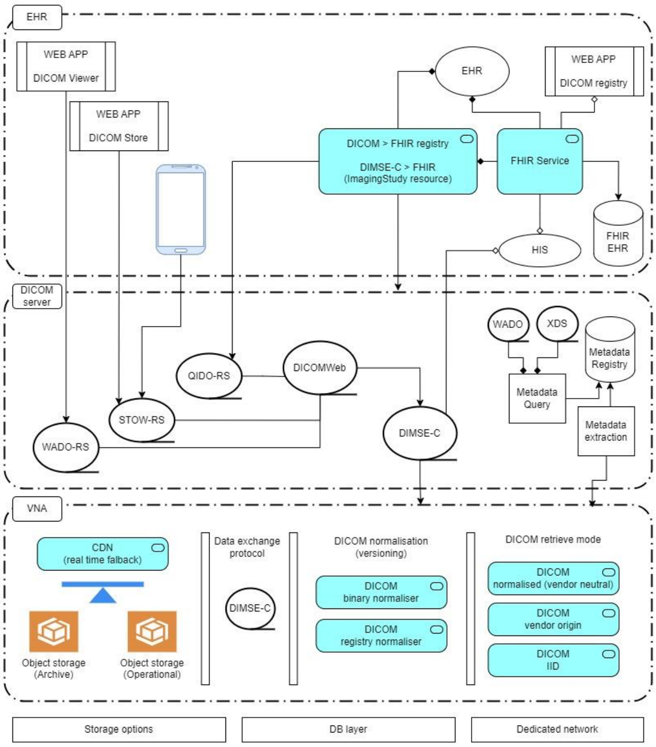

Figure 6. Diagram of the expected architectural components

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	Service provider: 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. Contracting Authority and technical supervision: 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)	MedVAIS_Priežiūra_ Sutrikimas
		Bug (to identify the cause and eliminate the issue)	
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)