**REQUIREMENTS FOR PROCUREMENT OBJECT**

**REQUIREMENTS SPECIFICATION FOR PUBLIC PROCUREMENT ESPBI IS POWERBI REPORTING PREPARATION SERVICES**

Table of Contents

1. Description and context 4

1.1. Project description and context 4

1.2. Terms and abbreviations 4

2. Scope of the project 4

2.1. Document purpose 4

2.2. Current situation 4

2.3. Establishing objectives and requirements 5

2.4. Required reports 5

3. REQUIREMENTS FOR SERVICE PROVISION 5

3.1. Project language 5

3.2. Requirements for documentation and its coordination 6

3.3. Requirements for project management 6

3.4. Requirements for change management 7

3.5. Ownership of the project results 7

3.6. Requirements for licencing 8

3.7. General project requirements 8

3.8. Implementation activities & results 9

3.8.1. Project timeline requirements 9

3.8.2. Initiation & general project management stage 9

3.8.2.1. General stage requirements 9

3.8.2.2. Responsibilities 9

3.8.2.3. Required stage results 9

3.8.3. Requirements analysis stage 10

3.8.3.1. General stage requirements 10

3.8.3.2. Responsibilities 10

3.8.3.3. Required stage results 11

3.8.4. Design stage 11

3.8.4.1. General stage requirements 11

3.8.4.2. Responsibilities 11

3.8.4.3. Required stage results 12

3.8.5. Development and configuration stage 13

3.8.5.1. General stage requirements 13

3.8.5.2. Responsibilities 14

3.8.5.3. Required stage results 15

3.8.6. Deployment to test environment stage 15

3.8.6.1. General stage requirements 15

3.8.6.2. Responsibilities 15

3.8.6.3. Required stage results 16

3.8.7. UAT stage 16

3.8.7.1. General stage requirements 16

3.8.7.2. Responsibilities 16

3.8.7.3. Required stage results 17

3.8.8. Deployment to production stage 17

3.8.8.1. General stage requirements 17

3.8.8.2. Responsibilities 17

3.8.8.3. Required stage results 17

3.8.9. Warranty stage 18

3.8.9.1. General stage requirements 18

3.8.9.2. Incident management 18

3.8.9.3. Support & maintenance 19

4. SPECIFIC REQUIREMENTS FOR THE PROVISION OF SERVICES 20

4.1. Safety requirements 20

4.1.1. Requirements for data protection and information security management 20

4.1.2. Requirements for the application of safety legislation 21

4.1.3. Data security requirements for the provision of services 22

4.1.4. Requirements for the security of user management 22

4.1.5. Audit requirements 23

4.2. Requirements for risk, threat and vulnerability management 23

4.2.1. Requirements relating to national security 23

4.2.2. Other safety requirements 24

5. Annex 24

5.1. List of required reports 24

TABLES

[Table 1. Terms and abbreviations used 3](#_Toc184146523)

[Table 2. Reporting creation activities 4](#_Toc184146524)

# Description and context

## Project description and context

1. The project focuses on modernizing and enhancing Lithuania's Electronic Health Services and Cooperation Infrastructure Information System (ESPBI IS), by improving current reporting capabilities. The maintenance of ESPBI IS is handled by the State Enterprise Centre of Registers (RC), while the Ministry of Health (SAM) is responsible for its governance and strategic decision-making. ESPBI IS serves as a central repository for health records and provides specific portals and subsystems used by both healthcare specialists and patients. This project will focus on improving current and adding additional reports within the system using existing tools. Reports are needed in 2 main domains (Informational system for registration of patients in advance (IPR); Informational system of pregnant, women in labor and newborns (NGN).

## Terms and abbreviations

1. Terms and abbreviations used are presented in table 1 “Terms and abbreviations used “.

Table 1. Terms and abbreviations used

| Term/abbreviation | Description |
| --- | --- |
| ESPBI IS | Electronic information system of health services and cooperation infrastructure (lit. *Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema*) |
| HIS | Healthcare information system |
| RC | State Enterprise Centre of Registers (lit. *Registrų centras*) |
| SAM | Ministry of Health (lit. *Sveikatos apsaugos ministerija*) |
| Client | State Enterprise Centre of Registers or RC |
| Service provider | The company that is providing software development services for the implementation of the project. |
| IPR IS | Informational system for registration of patients in advance |
| NGN IS | (lit. Nėščiųjų, gimdyvių ir naujagimių informacinė sistema) Informational system of pregnant, women in labor and newborns. |

# Scope of the project

## Document purpose

1. The purpose of this document is to provide a structure on possible reporting improvements in healthcare informational systems. These reports aim to guarantee standardization amongst the reporting of various healthcare institutions, accessible analytics.

## Current situation

1. Currently, the initial data from IPR IS, NGN IS is first stored in the Oracle database (ESPBI IS used Oracle database). Then data is transferred to Cloudera for further processing and transformations. After that data is transferred to centralized PostgreSQL database for reporting purposes.
2. For the reporting of IPR IS the data is taken from PostgreSQL and formatted into the reporting dashboards using PowerBI. One of the issues faced - the clarity of currently available reports. The project will aim to improve the quality of currently available reports by redesigning reports / dashboards and reformulating data queries to PostgreSQL database.
3. Tools for data reporting and data storing is owned by the Client and no tool needs to be provided. The data flow expected sequence should be as provided in the diagram below:

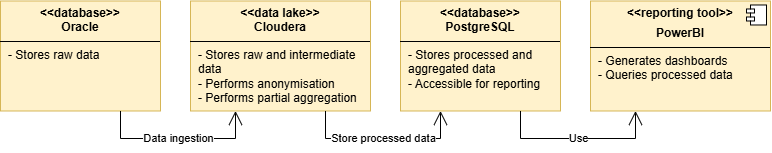


Figure 1. Data flow

## Establishing objectives and requirements

1. Goals and requirements of the project:
   1. Optimize the existing query processes and structure in the PostgreSQL database to enhance efficiency and ensure they accurately reflect current analytics by rewriting outdated queries and developing new ones.
   2. Design and implement new dashboards for the analytics and reporting of NGN and IPR data.
   3. Authorization must be managed within the portals. However, authorization rules must be propagated to Power BI to ensure that portal users can only access Power BI data according to the defined authorization rules. This must be achieved by implementing appropriate mechanisms such as Row-Level Security (RLS) or other suitable alternatives when generating embedded tokens. Service provider is responsible to designing and implementing authorization mechanisms.
   4. All reports shall be hosted and accessible through Power BI Cloud (Azure).
   5. Service provider shall calculate and provide estimation of how much additional capacity will be required from Azure.
   6. Reports shall be accessible from specialist and patient portal. Service provider is responsible for ensuring access to reports from these portals. The generated reports must be embedded into the existing client-managed portals.
   7. If modifications to the existing portals are necessary to grant access, create additional required menu items for reports, or implement other relevant functions to ensure proper report display, the necessary changes must be implemented directly in the portals by Service provider.

## Required reports

1. The project focus is on preparing the PostgreSQL based reports for 2 fields: Patients’ registration in advance (IPR), pregnant, women in labour and newborns (NGN). Required reports and their description is provided in the annexes (see [Annex 5.1. “List of available reports](#_List_of_available) “).
2. Access rights to different reports must be ensured based on professional qualification, healthcare institution or other criteria.
3. Reports are separated into priorities. First-priority reports will be automatically required, however other priority reports will be requested on demand.

# REQUIREMENTS FOR SERVICE PROVISION

## Project language

1. Project documentation must be prepared in both Lithuanian and English languages. Interim documentation (non-final) may be prepared in a single language, however all final deliverables must be provided in both languages.
2. Project communication can be held in Lithuanian or English languages.
3. User training can be held in Lithuanian or English languages.

## Requirements for documentation and its coordination

1. Client will review documentation, and the Service Provider shall adjust it constructively, arranging meetings if any remarks are unclear. Client may align the document internally based on its content, potentially involving cybersecurity, product owners, or other relevant parties in the review process.
2. All project documentation prepared by the Service provider must be prepared in accordance with the rules of the respective language grammar and formatting rules illustrated with diagrams, tables, graphs and other visual means, the presented material is arranged clearly, consistently and in detail.
3. Project documentation must be updated according to project stages, activities, and all approved decisions. Final versions must reflect any changes (even previously approved documents) unless agreed otherwise.
4. If a project has multiple streamlines (e.g., priority 1 reports are implemented first followed by others) each must comply with all requirements, including full documentation, unless agreed otherwise.
5. Project documentation must be stored and coordinated in the Client's Confluence environment, while project task management must be carried out in the Client's Jira environment. Access to these systems will be provided by the Client at the start of the project.
6. The Service Provider must align all document templates with the Client. While document structure may evolve during the project, they should be submitted at the beginning each document preparation phase to align initial expectations.
7. The final versions of the documents must be submitted electronically in a format suitable for editing (e.g., .doc, .docx, or another agreed format), including diagrams and other content, unless agreed otherwise. Diagrams must be prepared using the draw.io tool.
8. Where applicable, the Service Provider shall apply use cases prepared in UML, BPMN, or an equivalent notation.
9. Client and other relevant parties commit to reviewing the documentation and providing comments within no more than 5 business days (unless agreed otherwise).
10. The Client’s GitLab repository must be used to store the system source codes (if applicable).

## Requirements for project management

1. Service provider must cooperate directly with the Client, Project partners, project supervision 3rd party suppliers and other interested parties involved in the Project. This includes maintaining open lines of communication and collaboration throughout the project duration.
2. Service Provider must regularly update the Client on the progress of the Services by organizing status meetings and, upon the Client's request, prepare and present results at various stages of service delivery.
3. Not later than within 30 (thirty) calendar days from the date of entry into force of the Contract, the Service provider shall organize a kick-off meeting. The exact agenda of the Project kick-off meeting must be agreed with the Client at the beginning of the Project.
4. During the implementation of the Project, to organize working meetings/teleconferences of the Project team at least 1–2 times a week. After each meeting/teleconference, to document the decisions made using a protocol template provided by the Client or an action points register agreed at the beginning of the Project.
5. To assist the Client in the preparation of the materials for the meetings of the Project Steering Committee such as:
   1. To detail problems, possible solutions, alternatives. To prepare cost-benefit analyses and to make decisions on budget increases, where appropriate.
   2. To provide up-to-date summary information on the Project course, progress, etc.
6. To prepare all documents during the Project implementation taking into account the templates available to the Client or using the Client’s templates. To use other document templates only upon obtaining the Client’s approval.
7. Sharing of data, as well as documents created/under creation during the Project, shall take place through secure channels with or without encryption (password) protection. This shall be agreed with the Client at the beginning of the Project.
8. Considering that the client plans to implement not only this project but also additional projects simultaneously, the vendor must be prepared to allocate the necessary resources and participate in meetings to discuss inter-project interdependencies.
9. Project must be executed in accordance with recognized project management practices as SDLC, with a likely implementation of a hybrid Agile and Waterfall approach, ensuring that systematic planning, monitoring, and delivery methodologies are applied.

## Requirements for change management

1. Client reserves the right (but is not obligated) to order additional services from the Service Provider based on the hourly rate specified in the proposal. The scope of additional services is up to 175 working hours.
2. Service Provider must apply an hourly rate no higher than specified in the proposal. Before starting additional work, the Service Provider must provide a detailed task description, time estimates with justifications, and an implementation timeline, all of which must be agreed upon with the Client. The Client reserves the right to approve or reject the change request based on the evaluation. The preparation of the estimate must be done at the Service Provider's expense.
3. Service Provider must establish and agree with the Client on a detailed procedure for providing additional services, including rules for identifying, calculating, and documenting additional service orders.
4. These are preliminary types of possible additional services:
   1. Modifications for unforeseen areas or functionality.
   2. Additional training or consultations.
   3. Issues addressed during the warranty period that were ultimately determined not to be actual issues or fell outside the warranty scope, but still required the Service Provider’s time and effort.
   4. Other tasks agreed upon with the Client.
5. Service Provider must account for and include in their calculations all project documentation to be prepared or updated, along with any necessary modifications, to achieve the objectives of the change request.
6. Additional services are subject to the same warranty period as the System. If additional service results are delivered near the end of the warranty period, a minimum warranty of 2 months will apply to those results.
7. Service provider or Client may propose an alternative implementation method or equivalent functionality, ensuring no negative impact on tender objectives or legal compliance. Alternatives require Client approval. If substituting a requirement, the Service provider must justify the change in writing, assessing its impact, criticality, and time costs

## Ownership of the project results

1. All documents and/or information prepared or received during the provision of Project services must be transferred to the Client (including documents and information provided in electronic or digital format) and become the property of the Client, which may use them at its discretion. If a standard solution is proposed by the Service Provider, this requirement does not apply, and ownership rights do not transfer. In such cases, only the ownership of created custom modifications is transferred to the Client.
2. Service Provider must transfer the System's source code, developed during the project.

## Requirements for licencing

1. Licenses are not purchased in this procurement. The Client has allocated a budget (see the proposal submission form) to be used for acquiring additional necessary Azure resources. The Service Provider will be responsible for calculating and procuring the additional resources, but the total cost must not exceed the amount specified in the proposal submission form.

## General project requirements

1. Examples, attributes, criteria, parameters, rules, and classifiers mentioned in the requirements are indicative and not exhaustive. These must be detailed and agreed upon with the Client during analysis and design phases.
2. All necessary data fields for proper system functionality must be included, with character limits and integration methods agreed upon during analysis and design.
3. Solution must comply with current legal regulations (the ones that are valid at the date of the proposal submission).
4. Service Provider must align documentation with the Client and demonstrate system prototypes during analysis, design, and testing phases.
5. According to the specifics of the procurement object, the Service Provider's specialist may be granted access to the necessary database schemas for the execution of the procurement object.
6. Service Provider, together with the Contract, signs a personal data processing agreement.
7. Service Provider ensures that the person responsible signs the Confidentiality Commitment provided by the Client.

## 

## Implementation activities & results

## Project timeline requirements

1. All project services & deliverables (except for warranty) must be completed and submitted **within the time specified in the contract.**
2. Project initiation documentation shall be submitted no later than 10 business days after the contract signing.

## Initiation & general project management stage

## General stage requirements

1. Service provider must designate specific individuals responsible for executing the service provision contract and managing communication with the Client and the technical supervision service provider. The Client must be informed of these appointments within 2 business days from the date of signing the service provision contract.
2. Service provider must, within 2 business days, assign the project team and submit a list of required logins for JIRA, Confluence, or other necessary tools for the Client to provide.
3. Service provider must submit a list of open questions or required information from the Client within 10 business days of the service provision start date.
4. General results acceptance criteria:
   * 1. If no critical issues are identified and no more than 10 non-critical issues are identified UAT stage can be confirmed.
     2. If no critical issues are identified and no more than 5 non-critical issues are identified information system can be deployed to PROD environment.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Prepares documentation. | * Provides the necessary information; * Makes comments and recommendations. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Project initiation documentation | * Prepared project initiation documentation, detailing:   + Project objectives, goals & priorities,   + results (deliveries) description (the scope and results of the stages)   + stakeholders (interested parties)   + project team & responsibilities (detailing organizational structure of decision-making process)   + work schedule (detailed with milestones and buffer time)   + risks and their management methods,   + communication principles,   + criteria for interim and results acceptance,   + change management procedures. |
|  | Bi-weekly briefing report | * Prepared project initiation documentation, detailing:   + Project schedule status   + Relevant project risks   + Existing open questions   + Main activities done during last 2 weeks   + Main activities planned for next 2 weeks |

## Requirements analysis stage

## General stage requirements

1. Service provider shall organize meetings with Client representatives and review all relevant Client documentation. Each meeting must have a clear agenda, and topics for discussion must be shared in advance.
2. Service provider shall proactively offer insights and suggestions based on industry best practices.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Carries out an assessment of the current and desired situation; * Prepares documentation for detailed analysis; * Carries out other activities provided for during the analysis phase. | * Provides the necessary information; * Makes comments and recommendations; * Approves the presented results of the stage. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Requirements analysis report | * Prepared requirements analysis report, detailing:   + Description of each functional & non-functional requirement provided in the technical specification, unless agreed otherwise (some requirements might not require additional description). The purpose of the description is to align fully between Client and Service Provider on the objective of each requirement.   + Preparation of user stories and use cases, presented in the form of use case diagrams following UML (Unified Modeling Language) notation, with detailed descriptions of execution steps, including main course, alternative progress, and other restrictions. If necessary, descriptions of system users and their rights are also included.   + Insights on identified required change requests. |

## Design stage

## General stage requirements

1. Service provider shall configure the following solution environments unless otherwise agreed with the Client:
   * 1. Demonstration
     2. Training
     3. Testing
     4. Pre-production
2. All environments will be prepared by the Client. The service provider shall be responsible for configuring and deploying the system to all environments except for the production (PROD) environment, where deployment will be carried out by the Client.
3. Service provider shall review the Client’s existing infrastructure documentation to identify infrastructure requirements needed for the solution.
4. If the system architecture is developed during the project, the Service provider, upon the client's request, presents it to the client's architecture board and modifies it based on the received feedback. If necessary, additional presentations may be organized.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Performs design and prepares design documentation; * Analyse and prepare documentation describing the integration interfaces; * Aligns new integration interfaces with data providers and recipients; * Develop specifications for the integration interfaces and align them with the recipients and providers of the data and the Client. | * Provides the necessary information; * Makes comments and recommendations. * Approves the presented results of the stage. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Solution design report | * Prepared solution design report, detailing:   + Implementation and software configuration:     - Descriptions of requirements implementation, including functions, screens, rules, restrictions, and any additional functionalities beyond the specification.     - Clarification on whether requirements are implemented as part of the standard system or through modifications.     - Descriptions of system parameters and configurations.   + System architecture:     - System architecture diagram and component descriptions, detailing integration with the existing ESPBI architecture.     - Technologies used, including names and versions.     - Deployment view, illustrating the distribution of software components in hardware.     - Security, high availability, and scalability solutions.     - Technical architecture document covering key system components.   + Database architecture:     - Logical and physical database structure.     - Informative view, including database structures and interface diagrams.     - Developed logical database model.     - Built-in interface specifications, including developed interface and data exchange specifications.   + Functional & UX/UI Design     - Functional image, detailing system units, their functions, interrelationships, and UI prototypes.     - UX/UI design models, including:       * User interface diagrams.       * Structure and design.       * Initial user interface prototype.   + Integration and deployment:     - Integrative image, defining interfaces between internal and external systems.     - Detailed integration data, management, and deployment areas.   + Infrastructure requirements:     - Operational picture, describing system processes, algorithms, and periodic operations.     - Prepared technical specification of infrastructure requirements, covering:     - Technical and system software requirements for proper solution functioning.     - Analysis of additional hardware and software compatibility with the Client's existing infrastructure.   + Roles and permissions:     - Complete role and permission details, including a list of roles, their definitions, and purposes. |
|  | Testing scenarios (for UAT) report | * Prepared testing UAT scenarios report, detailing:   + Testing scenario, it is description and expected outcome   + Each functional & non-functional (unless agreed otherwise) requirement shall be related to testing scenario (-s), ensuring that whole functionality will be tested. |
|  | Infrastructure requirements report | * Prepared infrastructure requirements report, detailing:   + Required infrastructure need for solution deployment. |
|  | Solution environments report | * Prepared solution environments report, detailing:   + Description of each solution environment and its purpose.   + Responsibilities of the Client and the Service provider for environment management.   + Timeline indicating when each environment will be used.   + Plan for deployment into the test and other environment. |

## Development and configuration stage

## General stage requirements

1. Service provider shall prepare all development & configuration activities to prepare solution and achieve project objectives.
2. All development activities by the Service provider must be performed directly on Client servers.
3. Service provider shall conduct internal testing and ensure that solution provided for the UAT shall not have any significant bugs.
4. Data backup mechanism must be set up, and data recovery procedures must be documented and tested.
5. Service Provider must conduct internal testing of individual components without the participation of the Client's representatives. However, the Service provider must provide proof of such testing, including internal testing reports, automated test scripts uploaded to the Client’s GitLab version control system, and a list of identified discrepancies. Internal testing must be performed in the development environment. Automated tests must be integrated into the CI/CD processes. Internal testing activities must be conducted using test scenarios prepared by the Provider in the Client’s test management tool, XRAY.
6. Service Provider must develop automated testing and deployment processes for the System and its components using the Client’s GitLab platform for Continuous Integration and Delivery (CI/CD).
7. Service Provider shall conduct all necessary tests to ensure that the product meets the required quality and performance standards. The complete list of tests, which must be aligned with the Client, may include, but is not limited to:
   * 1. Unit Testing
     2. Integration Testing
     3. System Testing
     4. Regression Testing
     5. Functional Testing
     6. Non-Functional Testing
     7. Performance Testing
     8. Security Testing
     9. Usability Testing
     10. Compatibility Testing
     11. Installation Testing
     12. Configuration Testing
     13. Smoke Testing

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Carries out the necessary development and configuration tasks (in its own development environment), implements functional and non-functional requirements; * Performs unit testing, internal security testing, subsystem internal testing, interface testing with other systems; * Conducts demonstrations of the subsystem being developed, takes into account the comments made by the Client; * Prepares an internal testing report. | * Provides the necessary information; * Participates in demonstrations of the subsystem, provides feedback; * Reviews and evaluates the results of internal testing; * Makes comments and recommendations. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Internal testing report | * Prepared internal testing report, detailing:   + Comprehensive internal testing report, covering:     - Scope of testing.     - Execution methodology.     - Types of testing performed.     - Testing procedures.   + Insights or comments, where additional attention should be provided during UAT.   + Testing results for each testing scenario.   + Internal security testing results, including findings from security tests performed. |
|  | User manual (regular users) | * Prepared user manual (regular users), detailing:   + All user functionalities should include detailed step-by-step instructions, relevant screenshots, possible alternatives, and any additional necessary information. |
|  | User manual (admin users) | * Prepared user manual (admin users), detailing:   + Administrator instructions, as system configurations, data integration configuration, back-ups, etc. Service provider shall include relevant screenshots, possible alternatives, and any additional necessary information. |

## Deployment to test environment stage

## General stage requirements

1. System shall be deployed to test environment.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Prepares and submits the software suitable for installation in the Client’s testing environment; * Advises the Client on the implementation of the Client’s testing environment; * Prepares data loading scripts into the Client’s test environment; * Develops acceptance testing scenarios, testing methodology and plan; * Prepares instructions for users and administrators | * Reviews and evaluates the deployment plan; * Provides the necessary information; * Controls the testing environment; * Installs the submitted software into the Client’s testing environment; |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Deployment to test environment report | * Prepared deployment to test environment report, detailing:   + Description of how software was prepared and installed in Client’s testing environment.   + Testing scenarios, acceptance testing methodology, and plan developed and agreed with stakeholders.   + Test data prepared (SQL and/or other scripts).   + User manuals and administrator instructions developed. |

## UAT stage

## General stage requirements

1. Service provider shall participate in all UAT sessions, provide insights, consultations and recommendations.
2. System shall be installed into Client’s testing environment and configured.
3. Service provider is responsible to register all scenarios into Client’s internal issue management system (JIRA).
4. If a bug is registered, the Service Provider shall conduct internal testing and ensure regression testing of the related functionality before making it available for UAT again.
5. Service Provider must prepare sufficient test data to ensure that, during acceptance testing, the System contains enough imported test data to fully validate all newly developed or modified functionality. The import of the test data into the TEST environment will be performed by the Client’s representatives using the import tools (scripts, descriptions, or other means) provided by the Service Provider.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Actively participates in acceptance testing and provides consultations; * Fixes recorded defects (bugs); * Makes necessary adjustments based on Client’s penetration testing and performance testing results; * Prepares an acceptance test report; * Updates test scenarios as needed. | * Performs acceptance testing; * Provides the necessary information; * Submits additional relevant testing scenarios; * Provides feedback and recommendations. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | UAT report | * Prepared UAT report, detailing:   + All incidents (bugs / questions) registered during UAT and their status   + All testing scenarios tested and their status.   + Client may conduct penetration and/or performance testing and share the results with the Service provider. Service provider must resolve the identified issues by implementing the necessary changes and perform a re-testing of the fixed areas to confirm that all issues have been resolved. |

## Deployment to production stage

## General stage requirements

1. Service provider shall provide source code and detailed instructions for it.
2. Service provider shall ensure that the software is ready for installation in the production environment.
3. Service provider shall prepare the necessary data for production operation in the form of SQL and/or other scripts.
4. Service provider shall coordinate the launch plan for the new functionality with all data recipients and providers.

## Responsibilities

| Service provider’s general responsibilities | Client’s general responsibilities |
| --- | --- |
| * Prepares software for deployment to PROD. | * Deploy information system to PROD environment. |

## Required stage results

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | PROD deployment plan | * Prepared PROD deployment plan, detailing:   + Roles of Client and Service provider for deployment process.   + Requirements (implementation guide) for external information systems (if applicable).   + Deployment schedule.   + Detailed description of installation activities.   + Structured installation scheme. |
|  | PROD deployment report | * Prepared PROD deployment report, detailing:   + Summary of the implemented solutions.   + Documentation of data structures, attributes, and data exchange processes.   + Description of the technical implementation, detailing the system's technical requirements and expansion capabilities.   + Any other relevant information. |
|  | Project insights & additional recommendations | * Prepared project insights & additional recommendations, detailing:   + Service provider’s insights for project related aspects, as identified related risks, recommendations for future developments (projects). |

## Warranty stage

## General stage requirements

1. Service Provider must ensure warranty for the developed solution and installed licensed software.
2. Warranty does not cover changes made by Client itself.
3. Warranty period is 12 months from the signing of the final delivery-acceptance act.
4. If the solution is delivered and implemented in parts (not as a full scope), the warranty will apply separately to each part upon its deployment. However, the overall warranty for the entire solution will start upon final deployment and remain valid for the full specified warranty period.
5. Service Provider must coordinate a detailed warranty maintenance procedure with the Client before the beginning of warranty period.

## Incident management

1. Critical incidents. System failures, critical function malfunctions, or issues such as security breaches or data corruption.
2. Non-critical incidents. Minor disruptions, cosmetic errors, or issues with potential workarounds.
3. Incidents must be recorded and monitored in the Client's issue management software, JIRA.
4. Incident management must be handled according to the table below:

| Aspect | Rule for the first 2 months | Rule for the remaining 10 months |
| --- | --- | --- |
| Applicable period | First 2 months of the warranty period | Remaining 10 months of the warranty period |
| Relevant operating hours | 24/7, including weekends, public holidays, etc. | Warranty service must operate from 08:00 to 18:00 (Lithuanian time zone), considering the client's working days |
| Critical incident response time | Must be responded to within 2 hours | Must be responded to within 2 working hours |
| Non-critical incident response time | Must be responded to within 4 hours | Must be responded to within 4 working hours |
| Critical incident resolution time | Must be resolved within 1 day | Must be resolved within 1 working day |
| Non-critical incident resolution time | Must be resolved within 10 days | Must be resolved within 10 working days |

## Support & maintenance

1. Support via phone and email ("Hotline") must be available during the Client's working hours, i.e., from 08:00 to 18:00 (Lithuanian time zone), considering the Client's working days. Only Level 2 hotline support must be provided, while the Client will ensure Level 1 support.
2. Updates to system source code must be provided for Client review after corrections are made.
3. During the warranty period, the Service Provider must update the software if a new version becomes available.

| Result no. | Result name | Result description |
| --- | --- | --- |
|  | Warranty plan | * Prepared warranty plan, detailing:   + Roles and responsibilities of Client and Service provider.   + Procedures of communication (channels, tools, etc.). |
|  | Warranty report | * Prepared warranty report, detailing:   + All incidents registered during warranty and their status.   + All change requests (for all project long) and their status. |

# SPECIFIC REQUIREMENTS FOR THE PROVISION OF SERVICES

## Safety requirements

## Requirements for data protection and information security management

1. Data safety must be ensured in accordance with the Data Security Regulations of the IS, the protection of personal data must be ensured on the basis 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 by which repealing Directive 95/46/EC (General Data Protection Regulation).
2. The Provider must ensure compliance with 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, the 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 Description of general requirements for electronic information security, Description of the guidelines for the content of security documents T-29 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", and other relevant legal requirements including government resolutions on electronic information security.
3. After the completion of the ESPBI IS Purchase activities, the data stored in the ESPBI IS must be protected from unauthorized access, use, alteration, disclosure, destruction or loss.
4. Personal data transmitted through public data transmission channels must be encrypted.
5. It is forbidden to make personal identification numbers publicly available.
6. The ESPBI IS must ensure the correct management of emergency situations caused by incorrect user actions or other information system issues. Users or systems must be informed about the occurrence of such a situation and possible further actions.
7. Measures must be implemented to trace activities of system users through the System interface, with audited data specifics to be coordinated with the Buyer during analysis and design phases
8. To prevent excessive accumulation of audit information, moments for making audit records must be identified during detailed analysis in collaboration with the Buyer.
9. In the event of ESPBI IS malfunctions, appropriate notifications must be provided to users.
10. When designing modifications for the ESPBI IS, the Provider must coordinate with the Buyer on protections for specific functionalities to safeguard against various threats:
    1. Security vulnerabilities such as unauthenticated access and software vulnerabilities must be addressed;
    2. Unauthorized user session interception;
    3. Unauthorised interception or insertion of data;
11. Insertion of harmful code, including Injection attacks and Cross-Site Scripting (XSS);
    1. Other security breaches as listed in the Open Network Program Security Procurement (SSP) and documented by the Open Web Application Security Project (OWASP) at www.owasp.org.
12. Secure coding practices and standards such as those by OWASP must be adhered to in software development, ensuring no unauthorized data access or other security breaches.
13. Security checks (threat simulations, source code views, etc. security checks provided for in the 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 intrusion resistance testing, which must be carried out from electronic ones the independent service provider of the entity carrying out the development of the services (the 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).
14. The security of web services provided by the ESPBI IS must comply with the WS-S (Web Services Security) standards.
15. The Provider must use certificates provided by the Buyer to secure web services.
16. The Provider must immediately inform about electronic information security incidents observed in the Buyer's information technology infrastructure during the performance of the contract, inoperative or improperly functioning security measures, non-compliance with information security requirements, signs of criminal activity, information system security vulnerabilities, other important security events and, in agreement with the Buyer, take appropriate measures and actions to identify electronic measures and actions to identify the cause of the information security incidents, to avoid the associated risks.
17. When providing services in accordance with the requirements set out in the Agreement, the Provider shall implement appropriate organizational and technical measures to protect information from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing.

## Requirements for the application of safety legislation

1. The main security (both software and data) legislation that must be followed in the development of the ESPBI IS are:
   1. 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)), 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".
2. The Provider will be required to carry out a ESPBI IS conformity assessment in accordance with the above-mentioned legislation and submit a report on such an assessment, which must be agreed with the RC. The conformity assessment shall be carried out no later than the start of the test operation of the Solution.

## Data security requirements for the provision of services

1. 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.
2. The security requirements set out in the data security regulations of the registers and information systems managed by the Buyer, documents implementing the security policy, the description of the procedure for managing cyber and electronic information security incidents and other legal acts (and in cases where such requirements change or arise after the signing of the public contract of sale).
3. Data security must be ensured by:
   1. ensuring the integrity, availability and confidentiality of data.
   2. recording the actions performed by the system users with the data, including the search and revision of the data (the identified group of system users must be required to enter the reason and/or legal basis for the actions performed in the ESPBI IS).
   3. creating tools enabling the system Administrator to verify the actions of system users.
   4. 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 the groups and roles of system users must be drawn up at the analytical and design stage.
   5. the information stored may not be deleted by any other means or under any circumstances other than those provided for at the analytical and design stages).
   6. The provider must match the file formats that are allowed to be uploaded to the ESPBI IS and coordinate them with the Buyer (e.g. the attachment of potentially unsafe ones that can automatically launch (E.g., it must not be allowed to pin potentially unsafe ones that can automatically launch). Self-executive files).

## Requirements for the security of user management

1. The System must automatically terminate a user's work session after a period of inactivity defined by parameters and inform the user of the reason for the disconnection with a message. The system administrator must be able to change the value of the inactivity period setting.
2. The system usernames, passwords, and other personal data that are subject to data protection laws must be stored with proper enforcement of access control and information encryption.
3. The system must be able to divide users into separate roles with different rights of access to individual system functions. A system user shall be able to view and modify only the information and use only the functions that are defined by their access rights.
4. According to the requests made by a system user, only the data that they have the right to view must be displayed.

## Audit requirements

1. The use of all system components (user actions) and their operations must be audited.
2. Requirements for technical-level audits relate to auditing system-level events, data manipulations, configuration changes, and security-related operations. The technical-level audit ensures the ability to reconstruct data processing history, investigate security incidents, identify unauthorized actions, and analyze system problems.
3. General technical-level audit scope:
   1. User authentication events (e.g., login, logout sessions).
   2. Changes to system parameters or settings.
   3. Data-related database operations, including inserting, updating, deleting, and viewing data.
   4. Searches performed, including search criteria (phrases) used.
4. Technical-level data storage requirements:
   1. Who performed the action (user)
   2. When the action was performed (date and time)
   3. Which data objects were viewed
   4. Which search phrases were used
   5. User IP address
   6. Any additional technical information agreed upon during the analysis and design phases

## Requirements for risk, threat and vulnerability management

1. The ESPBI IS must include risk, threat, and vulnerability management:
   1. The Provider must follow recognized methodologies for the secure development of software, such as ISO/IEC 27034-1 or equivalent.;
   2. The Provider must ensure that all employees involved in the development of the software are familiar with methodologies for secure software development;
   3. The Provider must perform inspections to identify the main security risks and vulnerabilities of the Solution, as specified in the CWE/SANS Top 25 Most Dangerous Software Errors and the OWASP Top 10 Most Critical Web Application Security Risks, and eliminate any risks and vulnerabilities found. After verification and elimination, the provider must provide a declaration stating that upon completion of the development work, the Solution does not contain the risks or vulnerabilities listed in the CWE/SANS Top 25 and OWASP Top 10;
   4. The Provider must provide a list of all third-party components used in the Solution;
   5. The Provider must take appropriate action (i.e., reasonable effort) to ensure that third-party components meet the client's security requirements.
2. During the acceptance testing phase, pilot phase, or any other agreed-upon time, the provider shall provide all necessary conditions for client representatives who will conduct penetration testing. If necessary, the provider must perform configuration or programming work required to test the security of the Solution in various usage scenarios. The provider is not obligated to supply any software or hardware to run these tests.
3. The provider must carry out the necessary Solution programming and/or configuration work, considering the results of the penetration tests conducted by the client's representatives, to eliminate all identified significant security vulnerabilities before the Solution is put into operation.

## Requirements relating to national security

1. The Provider must ensure that the services offered comply with the requirements specified in the "Description of the Organizational and Technical Cybersecurity Requirements Applicable to Cybersecurity Entities," approved by Resolution No. 818 of the Government of the Republic of Lithuania dated August 13, 2018, "On the Implementation of the Law on Cybersecurity of the Republic of Lithuania“.
2. The Provider must sign an agreement on the processing of personal data as set out in Article 28(3) of Regulation (EU) 2016/679 (General Data Protection Regulation), which must determine the subject matter and duration of the processing of personal data, the nature and purpose of the data processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the Buyer.
3. The Provider is responsible for complying with the requirements of the occupational safety and health legislation in force in the Republic of Lithuania and other documents regulating occupational safety and health at work.

## Other safety requirements

1. Management of security patches and updates:
   1. The Provider must use the latest stable versions of the software and its patches/fixes for the development of the Solution. During the installation of the Solution into the production environment, it must be ensured that the Solution uses the latest stable versions of the software, if this does not change the essential principles of the ESPBI IS architecture and functionality as defined at the design stage. Versions of software components that are in the testing stage or have been officially announced by the software manufacturer as no longer supported, improved, or developed from a certain date (end-of-life products) must not be used.
2. Prevention of unauthorized access:
   1. Any unauthorized or undocumented remote or local access/accounts, or any secret (undocumented) functionality that may compromise the security of the System, is prohibited.
3. Secure configuration:
   1. The Provider must provide detailed instructions for configuring the security of the ESPBI IS and platform (operating system, database management system, middleware).
   2. The Provider must provide a list of platform components, system services, and ports necessary for the functioning of the system. All components that are not necessary for the Solution's functionality must be deactivated before the Solution begins operation.
4. Network architecture:
   1. Data flows between different levels must be documented, indicating the ports and protocols required for communication, and must be limited by firewalls.
   2. The external portal of the ESPBI IS must be in a network segment separate from the internal subsystems of the ESPBI IS.

# Annex

## List of required reports

