**IMPORTANT NOTE**

Any information included herewith and any information that may be received from interested suppliers is without commitment and prejudice.

The issue of this document does not constitute a commitment by MITA to issue a request for bids, award a contract, or pay any costs incurred in preparation of any information that may be submitted in response to this document.



**External resources**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**T046/22 - Expression of Interest**

**Date of issue: 4 July 2022**

**Closing date: 22 July 2022**

**Unclassified**

Malta Information Technology Agency, Gattard House, National Road, Blata l-Bajda HMR 9010 Malta

Telephone: (+356) 21234710 Facsimile: (+356) 21234701

Web Site: [www.mita.gov.mt](http://www.mita.gov.mt)

1. **Purpose**

The Malta Information Technology Agency (MITA) is a public agency vested with the responsibility of providing ICT infrastructure, systems and services to the Government of Malta. The Programme Management Department (PMD) is MITA’s software delivery arm and needs to increase the resource capacity of its project teams responsible for developing, maintaining and modernising Government’s core IT systems.

This Expression of Interest (EOI) is meant to explore how skilled and qualified IT resources can be outsourced to MITA to provide software development and design services on the existing (legacy) IT systems and modernised IT systems. This EOI outlines MITA’s desirable requirements for the engagement of the IT resources for the Social Security and Taxation project teams.

1. **Requirements**

Refer to **Annexes A and B** for the desirable skills requirements and responsibilities of the out-sourced resources indicated hereunder.

* 1. **Out-sourced Resources required for the Social Security project team**

The Social Security project team requires the provision of:

Team 1:

1 Solution Architect\*

1 front-end software developer

1 Back-end software developer

Team 2:

1 Solution Architect\*

1 front-end software developer

1 back-end software developer

*\* It should be noted that the Solution Architect shall have the role of a technical lead and also have software development responsibilities.*

* 1. **Out-sourced Resources required for the Taxation project team**

The Taxation project team requires the provision of:

Team 1:

1 Solution Architect\*

1 front-end software developer

1 Back-end software developer

Team 2:

1 Solution Architect\*

2 back-end software developers

*\* It should be noted that the Solution Architect shall have the role of a technical lead and also have software development responsibilities.*

* 1. **Common requirements applicable for both project teams**
		1. **Security**

The Economic Operator shall:

1. Accept requirements defined in the Security Schedule (vide **Annex C**).
2. Provide IT resources with a clean police conduct (from the respective country of residence) and provide proof of clean police conduct certificates at its own cost.
3. Have an Information Systems Security Policy in place. Additionally, have physical, administrative and technological security procedures in place to keep all information processed on behalf of MITA secure.
4. Provide training on IT security awareness to its IT resources.
5. Be ISO 27001 Information Security certified, or equivalent. (It will be the responsibility of the Economic Operator to prove that the standard quoted and submitted is equivalent to the standard requested.)
	* 1. **GDPR**

*Note:*

*MITA shall provide test, dummy or sanitised data to the IT resources. Nevertheless, it may be the case the IT resources may have access to personal data to carry out some duties especially in relation to legacy-related work.*

The Economic Operator shall:

1. Enter in a Data Processing Agreement with MITA (vide **Annex D**). Economic Operators outside the EU/EEA and adequate countries, shall need to also sign EU Standard Contractual Clauses.
2. Process personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (the ‘GDPR’), Data Protection Act (Cap. 586 of the Laws of Malta, and any subsidiary legislation.
3. Process personal data for the sole purpose of the provision of the services and protect it from unauthorised access, viewing, modification, destruction or disclosure.
4. Apply privacy by design when performing the assigned tasks.
5. Access and use the authorised environment/s provided by MITA from within the European Economic Area or authorized country and in no way copy or extract data from the authorized environment.
6. Seek MITA’s authorization to update or delete any data in development databases.
7. Use the VPN provided by MITA to access development environment that shall hold sanitized data or empty schema and test data.
8. Have a Data Protection Officer/Representative within the EU/EEA.
9. Have a Data Protection Policy including how to report data breaches to the Data Controller.
10. If any processing activities will be carried out by third parties (i.e. sub-processors), MITA needs to be informed and needs to be re-assured that the sub-processor will comply with MITA’s GDPR requirements.
11. Provide training on data protection to its IT resources.
	* 1. **Engagement model - Provision of out-sourced resources**
12. The provision of out-sourced resources shall be governed by the Laws of Malta.
13. Each out-sourced resource shall:
	1. Match all or most of the skills and experience required by MITA.
	2. Be exclusively dedicated to the project and work 40 hours per week.
	3. Work during MITA’s normal business working hours, Mondays to Fridays[[1]](#footnote-1).
	4. Work remotely.
	5. Be willing and available on-site in Malta for a definite number of days if requested by MITA (e.g. during on-boarding).
	6. Have a clean police conduct certificate.
	7. Perform the tasks assigned by the MITA project manager in adherence with the technical direction and other instructions as provided by the MITA project team. Refer to the IT resources’ generic list of tasks in **Annex B**.
	8. Participate in Scrum ceremonies and other meetings as may be required.
	9. Use MITA’s Microsoft Azure DevOps tool to elaborate further on assigned product backlog items and regularly update on task progress and completion. Additionally, use any other systems, tools and documentation as may be instructed by MITA. And specifically, the IT Resources shall utilize resources on MITA’s hybrid cloud as solely required for the purpose of the provision of the service and as directed by MITA.
	10. Check the quality of one’s work before submitting it.
	11. Keep communication with MITA project team regular and report progress regularly to the MITA Project Manager using the tools provided.
	12. Attend trainings or familiarisation sessions that MITA may offer relevant for the work assigned.
14. The Economic Operator shall:
15. Propose IT resources, either from its internal pool of resources or by directly recruiting from the labour market, who match MITA’s requirements for MITA’s consideration and approval.
16. Besides the IT resources, appoint a key contact person to represent the Economic Operator and liaise with MITA on contractual matters.
17. Provide IT resources and replace within a month from notification if required by MITA. In case replacements are not affected within a month, MITA may not use the total hours procured.
18. At its own cost, provide clean police conduct certificates of its IT resources.
19. Provide the IT resources with a standard workstation and software, and network. For information purposes, the below are the software licences that the IT resources shall require:
* Microsoft Office Suite including Visio
* Visual Studio Professional subscription complete with MSDN/Enterprise Subscription with MSDN \*
* A capable text editor (e.g. Notepad++)
1. Make an effort to retain the IT resources and nurture their talent through training.
2. Inform MITA promptly when an IT resource resigns or is no longer in a position to provide the services.
3. Invoice MITA on a time and materials basis in arrears on a monthly basis.
4. Each MITA project team shall:
5. Deploy all the required infrastructure, take the technical decisions and give the technical directions.
6. Provide access rights to the IT resources to the relevant IT systems and infrastructure to be able to deliver the services. Additionally, remove any access rights upon resignation or when resources are replaced.
7. Provide the non-standard software/subscriptions that the IT resources may require during the contract term.
8. Manage the project end-to-end including the technical leadership and decision-making, establish work priorities, assign work tasks to the IT resources[[2]](#footnote-2), and vet for acceptance of work deliverables.
9. Inform the Economic Operator about the products planned for the upcoming three months (or any other agreed timeframe) in advance upon which the IT resources will be working on together with the MITA project team. Such product list may be subject to change in case of change in the client’s priorities or further refined estimation of work. Such changes will be formally communicated with the Economic Operator.
10. Regularly monitor the IT resources’ performance and formally appraise on the basis of Timeliness, Completeness and Quality through Appraisal reports.
11. Communicate regularly with the IT resources and keep the Economic Operator informed about the IT resources’ performance.
12. Pay the Economic Operator on the basis of certified invoices within 60 days from receipt of invoice.
13. If the quality of work delivered by any IT resource is found to be non-compliant with MITA’s technical direction (e.g. practising the SOLID principles of object-oriented design and production of clean code), and after communicating such issues to the Economic Operator and IT resource without effective resolution or improvement, MITA shall have the discretion to ask for a replacement of the IT resource.
14. In case of legal/security/data protection breaches by any of the IT resources on the basis of sufficient evidence, MITA shall have the option of requesting the immediate removal of the IT resource in question or potentially terminating the contract, partially or completely, if it is considered a material breach of the Contract.
15. All Intellectual Property Rights delivered during the Contract Term are MITA’s sole and exclusive property and the use of the Intellectual Property by MITA cannot be restricted in any manner whatsoever.
16. All information exchanged between MITA and the Economic Operator and its IT resources during the contract term is to be treated as confidential.
17. **Submission of interest**

In response to this EOI, Economic Operators are invited to submit their interest to MITA by email to the Manager (Contracts and Legal) at cmd.mita@gov.mt up to the 22 July 2022 (end of business).

Submissions shall be valid for a period of 90 days from the final date for the submission of the Expression of Interest.

Any requests for clarifications shall be submitted by Economic Operators exclusively by email at cmd.mita@gov.mt up to the 15 July 2022. Responses to clarifications will be subsequently published to all participating Economic Operators.

All submissions shall be treated with strict confidence**.**

Economic Operators are to note that any eventual, potential contract with one or more Economic Operators shall be construed to be a Contract for Service with the Economic Operator/s (and not a contract of service with the IT resource/s proposed) in line with the provisions of the Public Procurement Regulations (Malta).

In their submission, Economic Operators are requested to succinctly and concretely answer if and how they can satisfy the above-mentioned requirements, using the following format:

|  |  |  |
| --- | --- | --- |
| **Ref** | **Question** | **Response** |
|  | *Social Security Project Team & Taxation Project Teams – Out-sourced Resource Requirements**(Refer to Section 2.1 and 2.2 of this document)* |
| 1.1 | a. How will the Economic Operator procure the required IT resources? (e.g. from internal pool of resources, recruitment from the labour market, with the help of out-staffing companies?)b. What is the time lapse (in terms of weeks) that the Economic Operator can commit to providing an IT resource from the time it is notified by MITA to do so? |  |
| 1.2 | From which region/country will the IT resources work? |  |
| 1.3 | Provide profiles or CVs for each IT resource as requested in this EOI.  |  |
| 1.4 | Specify the maximum number of IT resources that the Economic Operator can provide.  |  |
| *2* | *Security requirements**(Refer to Section 2.3.1 of this document)* |
| 2.1 | Can the Economic Operator satisfy all the security requirements referred in Section 2.3.1 of this document?If not, specify which requirements cannot be satisfied and explain why. |  |
| 2.2 | Provide proof of ISO 27001 certification (or equivalent) and any other relevant certifications. |  |
| 2.3 | Are there any additional assurances that the Economic Operator can provide with respect to security? |  |
| *3* | *GDPR requirements**(Refer to section 2.3.2 of this document)* |
| 3.1 | Can the Economic Operator satisfy all the GDPR requirements referred in Section 2.3.2 of this document?If not, specify which requirements cannot be satisfied and explain why. |  |
| 3.2 | Complete the GDPR Adequacy Questionnaire (applicable if Economic Operator is located outside the EU /EEAregion). |  |
| 3.3 | Are there any additional assurances that the Economic Operator can provide with respect to GDPR compliance?  |  |
| *4* | *Engagement model - Provision of out-sourced resources**(Refer to section 2.3.3 of this document)* |
| 4.1 | Is the Economic Operator in agreement with the engagement model and roles and responsibilities proposed for the Economic Operator, IT resources and MITA as referred in section 2.3.3 of this document?  |  |
| 4.2 | If there are any requirements that the Economic Operator finds unacceptable, state which and explain why.  |  |
| 4.3 | Specify any terms that the Economic Operator would like to propose for the engagement of the IT resources. |  |
| 4.4 | Provide concise information about three (3) reference case studies implemented by the Economic Operator in the last three years, whose work is similar to what is being requested.  |  |
|  |  |  |
| *5* | *Quote (any charges quoted shall be inclusive of all applicable taxes and charges, but exclusive of VAT. The VAT shall be chargeable, where appropriate, separately and at rates for the time being in force).*  |
| 5.1 | Complete Table 1 – Fee Schedule below to provide the applicable hourly rates for each IT resource depending on the contract term and specify any other expenses that the Economic Operator may charge in addition to the resources’ hourly rates, if applicable.  |  |

**Table 1: Fee Schedule**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Solution Architect(Hourly rate €) | Front-end developer(Hourly rate €) | Back-end developer(Hourly rate €) |
| Contract term of 1 year |  |  |  |
| Contract term of 3 years |  |  |  |
| Contract term of 5 years |  |  |  |
| Other expenses (Please specify the kind of expense, recurrence, and cost), if applicable |  |

#

# **Annex A – Out-sourced Resources: Desirable Skills**

**Skills Requirements – Solution Architect**

* Holds an undergraduate degree in an IT-related field (Malta Qualifications Framework level 6 or equivalent);
* Holds at least three (3) years of work experience in solution architecture and design;
* Holds a valid certification as evidence of a good level of English language proficiency, both written and verbal (e.g. English Matsec or ‘O’ level certification, TOEFL, IELTS, EFSET). The certification must clearly indicate a score that is officially recognised as a pass (or higher) by the certification body concerned;
* Possesses good knowledge of UML standards to enable completion of modelling and visualizations during the compilation of Requirements Analysis and Design of software/system artefacts;
* Possesses knowledge and skills in the extraction of business logic from existing software written in different technologies;
* Possesses knowledge and skills in the use of Git or any other source code versioning tool;
* Possesses knowledge and skills in the use of Azure Components: App Services and Azure Storage;
* Possesses knowledge of Azure Components: Azure Service Bus and Azure Application Insights;
* Proficient to write REST APIs;
* Possesses knowledge of the CQRS pattern;
* Possesses knowledge and skills in the use of ASP.NET Core or later version, C#, JSON, OpenXML, HTML5, Javascript and CSS;
* Proficient in Object-Oriented Design;
* Possesses knowledge and skills to:
	+ Write anti-corruption layers and other seams to prevent legacy code from influencing new parts of the application; and
	+ Write unit tests that are de-coupled from the system under test.
* Possesses knowledge and skills in the use of Entity Framework Core and is proficient to write data-access layers based on Entity Framework Code-First and the repository pattern.

**Skills Requirements – Software Developer (Front-End)**

* Holds an undergraduate degree in an IT-related field (Malta Qualifications Framework level 6 or equivalent);
* Holds at least three (3) years of work experience in software development and systems analysis;
* Holds a valid certification as evidence of a good level of English language proficiency, both written and verbal (e.g. English Matsec or ‘O’ level certification, TOEFL, IELTS, EFSET). The certification must clearly indicate a score that is officially recognised as a pass (or higher) by the certification body concerned;
* Possesses good knowledge of UML standards to enable completion of modelling and visualizations during the compilation of Requirements Analysis and Design of software/system artefacts;
* Possesses knowledge and skills in the extraction of business logic from existing software written in different technologies;
* Possesses knowledge and skills in the use of Git or any other source code versioning tool;
* Possesses knowledge and skills in the design of prototypes;
* Proficient in the use of ASP.NET CORE MVC, JQuery, HTML5 and Bootstrap;
* Possesses knowledge of C# and front-end frameworks (Angular or Blazor).

**Skills Requirements – Software Developer (Back-End)**

* Holds an undergraduate degree in an IT-related field (Malta Qualifications Framework level 6 or equivalent);
* Holds at least three (3) years of work experience in software development and systems analysis;
* Holds a valid certification as evidence of a good level of English language proficiency, both written and verbal (e.g. English Matsec or Ordinary level certification (Malta Qualifications Framework Level 3 or equivalent), TOEFL, IELTS, EFSET). The certification must clearly indicate a score that is officially recognised as a pass (or higher) by the certification body concerned;
* Possesses good knowledge of UML standards to enable completion of modelling and visualizations during the compilation of Requirements Analysis and Design of software/system artefacts;
* Possesses knowledge and skills in the extraction of business logic from existing software written in different technologies;
* Possesses knowledge and skills in the use of Git or any other source code versioning tool;
* Possesses knowledge and skills in the use of ASP.NET Core, REST API, C#, JSON, and OpenXML;
* Proficient in Object-Oriented Design;
* Possesses knowledge and skills to:
	+ Write anti-corruption layers and other seams to prevent legacy code from influencing new parts of the application; and
	+ Write unit tests that are de-coupled from the system under test.
* Possesses knowledge and skills in the use of Entity Framework Core and is proficient to write data-access layers based on Entity Framework Code-First and the repository pattern.

# **Annex B – Out-sourced Resources: Roles and Responsibilities**

The below roles and responsibilities apply for the Solution Architect, Software Developer (Front-end), Software Developer (Back-end) roles. It should be noted that the Solution Architect shall have the role of a technical lead and also have software development responsibilities.

|  |
| --- |
| **Project Kick-Off** |
| **Task** | **Task Description** |
| Understand and learn | Understand and learn about: * the existing IT systems (including technologies, infrastructure, architecture, business, logic, code, functionality, analysis of current documentation etc.). The execution of the respective legacy applications on an environment provided by the Contracting Authority shall also assist in accomplishment of this Task;
* how the existing IT systems will be transformed;
* how the MITA project team operates (including policies, procedures, standards, methodologies, templates, etc.) and services its client/s, amongst others; and
* the technologies that will be used for the modernization of IT system; amongst others.

The overall objective should be for the IT resources to be able to work independently and produce quality work by the requested deadlines with minimal need for re-work. |

|  |
| --- |
| **Design** |
| **Task** | **Task Description** |
| Understand high level design  | Participate and actively contribute in event storming sessions and any other activities that will be held to understand the high-level design, extract the relevant User Stories and draft the required components.  |
| Code Analysis | Analyse existing code to extract and document the existing business rules, validations, data dependencies and other technical aspects that need to be mapped to the desired low-level design in terms of domain entities and other components in the domain model. The outcome of code analysis shall be detailed functional specifications and acceptance criteria. |
| Detailed Design Specification | Refine high-level design into detailed design specification including: * 1. Expanding or extending methods/behaviours
	2. Referencing to Data Layer API and ACL
	3. Further component decomposition in line with implementation frameworks
	4. Reallocation of legacy code logic to new components
 |

|  |
| --- |
| **Legacy Transition Strategy** |
| **Task**  | **Task Description** |
| Legacy Code Dependency Assessment | Analyse the existing code base to understand the dependencies of the replaceable functionality to ensure that the scope includes all necessary components that would displace the existing code. |
| Legacy Transition Strategy  | Define the transition of legacy components by:* 1. Marking aspects that would be eliminated
	2. Identifying areas where parallel execution to modernized versions are necessary
	3. Specifying migration test required
 |

|  |
| --- |
| **Development and Testing** |
| **Task** | **Task Description** |
| UI Design | Create layout of information and the navigation structure of screens that are responsive and accessible. |
| UI Development | Develop UI components as per UI design. |
| Microservices Development | Develop Application Services and Domain Services including the development of unit tests.There will be products that mandate the Test-Driven Development (TDD) approach, while other products might not need this approach, unit tests must still be developed. It is understood that there may be functionality that does not mandate the creation of unit tests at all (for instance maintenance screens). The products mandating a TDD approach will be identified by the MITA Project teams and tagged accordingly during event storming sessions. IT resources should make use of the documentation provided by the MITA project team and code analysis in order to build the initial list of unit tests for validations. When developing unit tests, these are to be developed using the xUnit[[3]](#footnote-3), Autofixture[[4]](#footnote-4) and FluentAssertions[[5]](#footnote-5) nuget package tools, or other tools as instructed by MITA. |
| Development of Domain Entities, Aggregates and data ACL | Develop Domain Layer and Data Layer including Domain Aggregates, Repositories, DbContexts and data Anti-Corruption Layer (ACL). The ACL consists of creating an entity framework data model that maps to the underlying data structure, and a set of adapters that translate between Domain Aggregates and data model.IT resources shall be responsible to follow the technical direction, quality requirements and standards of the MITA project team to produce clean and easily maintainable codebase. The produced software artefacts have to be fit for purpose (as per business requirements) and must be well built to guarantee maintainability. Code reviews will guarantee that software artefacts are built well and that the modernized codebase ensures, amongst others:* inclusion of automated unit tests (as part of the Solution) wherever required
* development of short functions in strict adherence to the single responsibility principle (typically in the region of 5 to 20 lines of code depending on the nature of the function)
* the consistent use of dependency injection leading to a decoupling between business logic and, for instance, data access services
* strict adherence to the CQRS principle
* strict conformance to the SOLID principles of object-oriented design
* qualifies as “clean code” (code runs all tests, contains no duplication, expresses all the design ideas that are the system, expresses all the design ideas that are in the system, and minimizes the number of entities such as classes, methods, functions, etc)

Furthermore, IT resources shall be required to:* keep dependencies to a minimum to ease maintenance and ensure every class and function do one thing well;
* produce code that uses meaningful names, is easy to read and does what the reader expects it to do; and
* produce code that can be easily enhanced by someone other than the original author and there should be nothing obvious that one can do to improve it.

IT resources shall carry out re-works where the code produced fails to qualify as “clean code” and fails to meet the technical direction/quality/standards/good practices provided by the MITA project team following quality reviews. MITA shall take the necessary steps to on-board the IT Resources and explain what is expected of them to develop software artefacts that are both fit for purpose and well-engineered. During the contract term, regular communication between the MITA project team and the IT Resources shall also be key to ensure IT Resources understand what is required of them and to discuss any issues that may impede work getting done or expectations to be satisfied, and consequently reduce the instances where the finished artefact is not line with MITA’s requirements. |
| Integration testing | Document a comprehensive list of tests and perform component integration and end-to-end testing. The outcome of the modernized products must be the same as the one provided by the existing software. In most instances there will be an element of parallel running where outcomes of the newly developed modernized products are compared with the outcomes obtained from the existing software currently in place. The IT Resources may be required to write code to enable such parallel runs. Apart from the functional tests, IT Resources shall perform other tests related to performance, stability of the product (stress testing) and security. Software security tools shall be embedded in the pipelines as part of the development. Telemetry through logs may be used for these types of tests as well. |
| Test Cases for User Acceptance Testing | Prepare tests cases for users to perform User Acceptance Testing and assist users during the User Acceptance Testing if required.  |
| Resolution of vulnerabilities | Resolve any vulnerabilities discovered after the running of any security tests.  |

|  |
| --- |
| **Quality, Compliance and Legacy Exit** |
| **Task** | **Task Description** |
| Security Review | Review compliance to security requirements including static code analysis. |
| Code Review | Carry out code reviews to ensure work is produced in adherence with:1. Coding Standards
2. Industry best practices
3. Architecture principles
* Data architecture
* Microservices architecture
* Web user interface architecture
* Application monitoring and logging architecture
* Application security
* DevOps processes and automated testing
 |

|  |
| --- |
| **Other** |
| **Task** | **Task Description** |
| Integration within the PMD team/s | Integrate within the MITA project team and consistently share one’s own knowledge and experience with the other team members to give added value beyond performing the tasks assigned by the MITA Project Manager (or his delegate). |
| Use of tools and environments | Use the tools and environments as instructed by MITA to perform the tasks. For instance, IT Resources shall:1. Use the source code repository provided by MITA to store all software related artefacts produced under this Contract; and
2. Be disciplined in creating and maintaining tasks in the Microsoft Azure DevOps; amongst others.
 |
|  Documentation | Prepare any documentation using the templates indicated by MITA or as may otherwise be instructed by MITA.Any documentation is to be prepared in the English language. This also applies to any source code and technical artefacts.Continuously update the artefacts provided by MITA in the structure as instructed by MITA, throughout the software development lifecycle to ultimately reflect the low-level Solution design reflecting the implementation.  |
| Interactions with stakeholders | Attend meetings (internal with MITA project teams, external with MITA Clients, or other stakeholders as the task may require) as may be required to complete tasks assigned, including assistance in walkthroughs and user acceptance sessions.  |
| Reporting | Diligently and regularly inform and keep updated the MITA Project Manager (or his delegate) about progress on tasks assigned and alert in a timely manner when any issues or difficulties arise which may impact the ability to deliver. |
| Compliance with Data Protection | Process personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (the ‘GDPR’), Data Protection Act (Cap. 586 of the Laws of Malta, and any subsidiary legislation, and the **Annex D** Data Processing Agreement. Also, process data for the sole purpose of the Contract and protect the data from unauthorized access, viewing, modification, destruction or disclosure. Furthermore:* 1. apply privacy by design when performing the assigned tasks as applicable;
	2. utilize the authorized environment/s provided by MITA from within the European Economic Area or authorized country and in no way copy or extract data from the authorized environment; and
	3. seek MITA’s authorization to update or delete any data in development databases; and
	4. use the VPN provided by MITA to access development environment that shall hold sanitized data or empty schema and test data.
 |
| Compliance with Security Requirements | Apply security by design when performing the assigned tasks and secure data in accordance with **Annex C** (Security Schedule). |
| Generic | Perform any other related tasks as instructed by MITA throughout the Contract term.All assigned tasks are to be performed to the best of one’s skills and abilities as instructed by MITA and in compliance with the policies, procedures, processes, standards, and regulations to which MITA adheres to meet its clients’ needs, as well as in adherence with the Contract.  |

**Annex C – Security Schedule**

1. **Definitions**

In this Schedule, unless the context otherwise requires the following expressions shall have the meanings set out below

|  |  |
| --- | --- |
| Breach of Security | includes the occurrence of unauthorised access to or use of the Customer Premises and/or the Location, the Services, the Solution or any ICT or data (including the Customer’s Data) used by the Customer or the Contractor in connection with the Agreement. |
|  |  |
| Adapters | Logical segregators which vary in shape and form, ranging from in-house developed software, off-the shelf software or specialised devices / environments (including firewalls, VLANs) as well as specific commercial arrangements etc. |
|  |  |
|  |  |
|  |  |

1. **Principles of Security**
2. The Contractor acknowledges that the Customer places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Location and the security for the Solution. The Contractor also acknowledges the confidentiality of Customer Data.
3. The Contractor shall at all times ensure that the level of security employed in the provision of the Services is in accordance with best industry practices and the applicable law, and is appropriate to maintain the following at acceptable risk levels (to the satisfaction of the Customer):
4. loss of integrity of Customer Data;
5. loss of confidentiality of Customer Data;
6. unauthorised access to, use of, or interference with Customer Data by any person or organisation;
7. unauthorised access to network elements, buildings and tools used by the Contractor in the provision of the Services;
8. use of the Solution or Services by any third party in order to gain unauthorised access to any computer resource or Customer Data; and
9. loss of availability of Customer Data due to any failure or compromise of the Services;
10. **Security Requirements**

The Contractor shall have the following responsibilities.

The Contractor shall abide by the provisions of the GMICT Information Security Policy available at <https://mita.gov.mt/en/GMICT/Pages/GMICT-Policies.aspx>.

**03.1 General**

1. Safeguard the confidentiality of data in accordance with Clause (12) (Confidentiality of Data) and ensure that the integrity and availability of the data that the Contractor manages and/or is responsible for by virtue of the Agreement is not compromised.
2. Ensure that it does not carry out and procure that its employees and subcontractors shall not carry out any act or omission which has or could reasonably be expected to have an adverse impact on the security of the Solution and the Customer’s business, activities, customers or systems.
3. Protect the integrity of the Solution and any data and/or information processed by the Solution during the provision of the Services.
4. The Customer reserves the right to undertake periodic reviews to assess the security status of the Solution and to ask any rectifications thereof as part of the tasks/services requested from the Contractor.
5. If applicable, ensure that resources external to the Solution are accessed through Adapters. Upon request by the Customer, the Contractor shall provide a report listing the resources outside the Solution that are being accessed by the Solution and the tools being used for such access.
6. Review and keep updated all security requirements indicated in this Schedule.
7. Immediately notify the Customer of any security breach of any one of the security requirements listed in this Schedule that the Contractor becomes aware of.
8. Pursuant to the circumstances referred to in the preceding clause:
9. take all reasonable steps necessary to remedy the breach or protect the Solution against any such potential or attempted breach or threat to prevent an equivalent breach in the future. The Customer reserves the right to make recommendations on the necessary steps to be taken. In case of changes required by the Customer that are not reasonably covered by the obligations of the Contractor under the Contract, the parties shall agree in writing as detailed in Clause (-) Amendments.
10. as soon as reasonably practicable, provide the Customer with the full details (using such reporting mechanism as specified by the Customer from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.
11. The Customer reserves the right to install further information security tools on the Solution to enhance the Protection, Detection and Response of such systems.

* 1. **Information Security Policy**
1. The Contractor shall possess an Information Security Policy which:
2. Is endorsed by senior management;
3. Is communicated to all the organisation’s employees and relevant external parties;
4. Is reviewed at planned intervals or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness;
5. Affirms management’s commitment and sets out the organisation’s approach to managing information security;
6. Highlights the security policies, principles, standards, and compliance requirements of the organisation;
7. Highlights responsibilities of the organisation’s senior management and employees vis-a-vis information security; and
8. Highlights the organisation’s approach towards protecting the confidentiality, integrity and availability of information it manages/operates/comes into contact with.
	1. **Security of Customer Data**
9. Ensure that Customer data shall not be stored outside the Solution, if applicable, without the Customer’s prior approval. Where the Customer provides approval, any transition of Customer Data outside the Solution shall be carried out using a communication method which is commensurate with the classification of the data, as identified by the Customer. Furthermore, the storage of any personal data shall be in line with the Data Processing Agreement as detailed in Schedule C.
	1. **Security in Third Party Agreements**
10. Procure from its sub-contractors involved in the provision of the service under the Agreement an undertaking to be bound by the same terms and conditions of the Agreement, including but not limited to the security requirements set out in this Schedule. This Clause shall be without prejudice to the responsibility of the Contractor to provide the Services under this Agreement.
	1. **Asset Management**
11. Ensure that the assets in use by the Contractor to provide the Service are maintained in an asset inventory that needs to be accurate, up to date, consistent and aligned with other inventories, where applicable.
12. With reference to cloud assets (i.e. a resource or policy configured or deployed onto a cloud-based environment) hosted on the Customer’s cloud services, the Customer inventory shall account for information and assets stored on the cloud computing environment at the resource group level.
13. Return all Customer-owned assets within a contractually established period upon termination of employees and/or expiration of the Agreement.
14. Protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, regulatory, contractual and business requirements. Examples of records are logs and/or reports created by information systems, asset inventories etc.
15. Apply disposal controls for the secure disposal or reuse of resources. Such controls are applicable to all media irrespective of warranty and including damaged equipment. Such controls shall be commensurate with the sensitivity of the data, as identified by the Customer. Verify all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
16. For the purposes of secure disposal or re-use, equipment containing storage media that might possibly contain personally identifiable information (PII) shall be treated as though it does.
	1. **Human Resource Security**

1. Return upon expiry or termination of the Agreement any credentials, keys, tokens and other similar devices required/used for the provision of the Service pursuant to the Agreement. Return the same in relation to Contractor Personnel that cease to provide a service on the Agreement.
2. Ensure that access rights granted to Contractor Personnel are removed upon expiry or termination of the Contract or otherwise upon in relation to such Contractor Personnel that have been replaced.
	1. **Information Security Awareness and Training**
3. Provide training on a continuous basis to Contractor Personnel involved in the provision of the Services in relation to the security requirements listed in this Schedule, including training on security awareness. The Contractor shall also ensure that it provides Contractor Personnel with access to documented operating procedures detailing the process carried out by the Contractor pursuant to the Agreement.
	1. **Physical and Environmental Security**
4. Ensure that physical controls are in place to prevent unauthorised access to Contractor premises if Contractor Personnel work at the Contractor’s premises
5. Ensure that Customer Data are stored in a secure manner and physically protected from unauthorised access and damage. Personal data shall be stored in accordance with the Data Processing Agreement as detailed in Schedule C.
6. Ensure that media containing information is protected against unauthorized access, misuse or corruption at all times.
7. In the case of Contractor personnel working remotely elsewhere other than the Customer’s premises, the required security measures, shall be applied to off-site assets including Contractor equipment (i.e. assets not located within premises managed by the Customer) taking into account the different risks involved to ensure that personally identifiable information is not accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).
	1. **Protection from Malware**
8. Set up protective mechanisms to ensure that the Contractor equipment used to provide the Service including any patches, updates or upgrades provided through any electronic media by the Contractor do not include harmful electronic data (including malicious code) which causes, or is likely to cause, detriment or failure or loss of performance, or loss of service, or harm in any degree to any computer systems or network systems owned by the Customer or other Third Parties.
9. Ensure that Contractor equipment used to provide the Service are patched regularly and installed with the latest updated version of end-point security software. The Contractor shall also implement lockout mechanisms on such Contractor equipment and regulate the use of Contractor equipment (including laptops) outside Contractor premises.
10. Ensure that the Contractor equipment used to provide the Service are protected by end-point security software compatible with the Solution. The Contractor shall be responsible to install and configure the end-point security software and to;
11. ensure regular updating of virus definition files;
12. ensure regular scanning of the relevant Contractor equipment;
13. update the virus signature file before each login, at least once a week; and
14. ensure cleaning of malicious code.
15. In case the Contractor Personnel operate outside the authorised environments provided by the Customer, ensure that operating systems are hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.
16. Implement detection, prevention and recovery controls to protect against malware, combined with appropriate user awareness.
	1. **Exchange of Information**
17. Set-up and maintain information handling procedures to ensure that the method chosen to exchange communications is commensurate with the sensitivity of the information exchanged, as identified by the Customer. For such purpose the Contractor shall have mechanisms in place to send and/or receive encrypted emails, to manage portable devices securely and to deliver sealed envelopes by hand rather than by post, amongst others.
	1. **Clock Synchronisation**
18. Ensure that clocks are synchronized with an accurate time-source.
	1. **Access Control**
19. Ensure that access rights on the contractor equipment and/or any Solution used for the provision of the Services are granted according to the ‘least-privilege-required’ principle. For such purpose, the Contractor shall enable audit logs to monitor and review access rights regularly. The Contractor shall also undertake to immediately disable user-accounts of Contractor Personnel that cease to provide a service on the Agreement.
20. Ensure that access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.
	1. **Account Management**
21. The Contractor shall not use generic accounts, unless with the prior written approval of the Customer. Named accounts shall be assigned to individual personnel. If more than one individual has access to stored information, then they shall each have a distinct account for identification, authentication and authorization purposes.
22. In case of use of generic accounts by the Contractor to operate and manage the Solution, as approved by the Customer, provide the Customer with the procedure the Contractor shall use to handle, store, access and change passwords. The Customer shall review the details submitted and may request the Contractor to revise such procedures to ensure an effective way of securing passwords.
23. Ensure that an account is not transferred from one person to another.
24. Ensure that disabled or deleted accounts are not assigned to other individuals.
25. Adopt a ‘least privilege principle’ approach throughout the management and use of accounts unless specific circumstances mandate otherwise. In the case of specific circumstances, the Contractor shall substantiate the reasons thereof.
26. The Contractor shall ensure that an account is deleted as soon as an employee is no longer working on the Solution.
	1. **Passwords**
27. Passwords used on all Solutions should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers.
28. Implement measures to safeguard against the sharing of passwords between Contractor personnel and implement controls to safeguard the confidentiality of passwords stored in a password management system.
29. Ensure that all personal computers utilised by the Contractor personnel are password protected to prevent unauthorised access.
	1. **Clear-desk and clear screen**
30. Ensure that papers and storage media containing Customer Data are stored in a secure manner (e.g. in locked cabinets) when not in use to reduce risks of unauthorised access, loss or damage to the Customer data.
	1. **Connecting to MAGNET**
31. In the event that the Contractor requires remote access to the Solution, network connectivity shall be provided through a Virtual Private Network (VPN) using strong two factor authentication. The VPN solution may be provided by the Customer or otherwise provided by the Contractor as part of the provision of the Solution. Where the VPN solution is to be provided by the Contractor the VPN solution shall be reviewed by the Customer for acceptance, in order to safeguard the integrity of its network.
32. MITA reserves the right to disconnect the system from MAGNET, if it is determined that the system is posing a security risk on the underlying infrastructure.
	1. **Teleworking**
33. Ensure that in cases where Contractor Personnel work outside Contractor premises appropriate security measures are implemented.
	1. **Protection of Production data**
34. Ensure that test data is used for testing purposes. Where test data cannot be used, the Contractor shall with the prior approval of the Customer use live data that is sanitised or, only where strictly necessary, use live data on a test environment that shall have the same level of security controls as in the operational environment. The Contractor shall delete any live data once testing is completed and shall inform the Customer in writing of such deletion for audit trail purposes.
35. Where applicable, segregate production and non-production environments to prevent unauthorized access or changes to information assets.
	1. **Operational Procedures and Responsibilities**
36. Ensure that data, including temporary data, is retained as per the retention period established and communicated by the Customer.
	1. **Control of technical vulnerabilities**
37. Implement measures to detect and manage technical vulnerabilities in the equipment in use by the Contractor for the provision of the Service in order to reduce risk from exploitation of technical vulnerabilities.
	1. **Information Security Incident and weakness management**
38. Set-up and maintain procedures to monitor, report and manage security incidents and security weaknesses.
39. Provide accurate information in a timely manner in the case of an investigation or security breach.
40. Note and report to the Customer any observed or suspected information security weaknesses in systems or services governed through this Agreement.
	1. **Information Security Reviews**
41. Regularly review information systems for compliance with :
42. the Contractor’s information security policy;
43. the GMICT Information Security Policy; and
44. the provisions of this Security Schedule and other technical direction as may be provided by the Customer.

In case of any conflict amongst the above, the GMICT Information Security Policy and the provisions of this Security Schedule and the Customer’s technical direction shall over-rule.

* 1. **Acceptable Use**
1. Ensure that the installation and use of utility programs that might be capable of overriding systems and application controls are restricted and tightly controlled. The Contractor shall ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorised personnel, and that the use of such programs is reviewed and audited regularly.

**Annex D – Data Processing Agreement**

**Preambles**

* + 1. Where the Data Processor requires the Sub-processor to provide the Data Controller with data processing services as part of the obligations of the Sub-processor pursuant to this Agreement.
		2. Whereas the Sub-processor is willing to provide these Services to the Data Controller.
1. **Definitions**

**‘Business Purpose/ Purpose’** means the purpose/s specified in Annex A (Purposes for which the Data Processor may process Personal Data).

**‘Confidential Information’** means such data as defined in Clause 6 of this Schedule.

**‘Data Protection Legislation / Data Protection Regime’** means the General Data Protection Regulation (EU) 2016/679 (GDPR), and the Data Protection Act 2018 (Cap 586) on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data whether held electronically or in manual form.

**‘Data Controller / Controller’** shall have the same meaning of ‘controller’ as set out in the GDP Regulation.

**‘Data Loss Event’** means any event that results, or may result, in unauthorised access to Personal Data held by the Data Processor under this Schedule and/or actual or potential loss and/or destruction of Personal Data in breach of this Schedule, including any Personal Data Breach.

**‘Data Processor / Processor’** shall have the same meaning of ‘processor’ as set out in the GDP Regulation.

**‘Data Processor System’** means the information and communication technology used by the Data Processor in the provision of the Service.

**‘Data Protection Impact Assessment’** means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**‘Data Subject’** shall have the same meaning of ‘data subject’ as set out in the GDP Regulation.

**‘Data Subject Access Request’** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

**‘Personal Data’** shall have the same meaning of ‘personal data’ as set out in the GDP Regulation.

**‘Personal Data Breach’** shall have the same meaning as set out in the GDP Regulation.

**‘Process’** shall have the same meaning of ‘processing’ as set out in the GDP Regulation.

**‘Protective Measures’** means the measures to be taken by the Data Processor in line with Article 32 of the GDP Regulation to protect against Personal Data Breaches, including technical and organization measures which may include pseudonymizing and encrypting, measures to ensure confidentiality, integrity availability and resilience of systems and services, and measures to ensure that availability of and access to Personal Data can be restored in a timely manner after an incident, and measures to regularly assess and evaluate the effectiveness of the measures adopted by it.

**‘Service’** means the service to be provided by the Contractor to the Customer as detailed in the main Contract.

**‘Sub-processor’** means any third party appointed by the Data Processor to process Personal Data on behalf of the Data Controller related to the Contract.

 **‘Software’** shall have the same meaning as defined in the Contract.

1. **Purpose of the Agreement**
2. The purpose of the Data Protection Agreement is to regulate rights and obligations in relation to the applicable Data Protection Act 2018 (Cap 586) of the laws of Malta and EUs General Data Protection Regulation 2016/679 of 27 April 2016 (“GDPR”).
3. The Data Protection Agreement governs the processing of personal data by Sub-processors on behalf of Data Processors, including the collection, registration, compilation, storage or disclosure of personal data, or combinations thereof, in connection with this project as detailed in this Contract ("Main Service Contract Agreement").
4. Sub-processor understands that the Data Processor **acts on behalf of a Data Controller** for the personal data covered by the agreement, and that Sub-processor are subject to similar obligations as the Data Processor is required by the Data Controller in accordance with Article 28 (4) GDPR.
5. The agreement shall ensure that personal data is not used illegally, unlawfully or that the information is processed in ways that lead to unauthorised access, alteration, deletion, damage, loss or inaccessibility. In the event of a conflict, the terms of this agreement shall precede the privacy statement of the Sub-processor, or the terms of other agreements entered into between the Data Processor and the Sub-processor in connection with the main agreement.
6. It must be stated in Annex II to the agreement if the Sub-processor can use its own sub-contractors under the Agreement, including for storage, processing or other use, cf. clause 9.
7. The purpose of the processing, the types of processing activities, categories of data subjects and the types of personal data that will be processed are set out in Annex I of this Agreement. These conditions cannot be changed by either party without a new agreement or an amendment to the agreement being signed by the Data Controller.

## Processing

* 1. The Sub-processors shall follow the written and documented instructions for the processing of personal data that the Data Processor has decided to apply.
	2. Sub-data processors undertake to comply with all obligations in accordance with the applicable personal data legislation applicable to the processing of personal data.
	3. Sub-processor undertakes to notify the Data Processor if the Sub-processor receives instructions that violates the privacy regulations.

## The Rights of Data Subjects

4.1 The Sub-processor shall notify the Data Processor immediately if it:

* + 1. receives a Data Subject Access Request (or purported Data Subject Access Request);
		2. receives a request to rectify, block or erase any Personal Data;
		3. receives any other request, complaint or communication relating to either Party’s obligations under the Data Protection Legislation;
		4. receives any communication from the Data Protection Commissioner or any other regulatory / supervisory authority in connection with this Schedule; and
		5. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purports to be required by law.
	1. The Sub-processor is obliged to assist the Data Processor in the treatment of the data subject's compliance with the data subject's rights in accordance with data protection legislation.
	2. The data subject's rights include the right to information on how his or her personal data is processed, the right to demand access to his own personal data, the right to demand rectification or deletion of his personal data and the right to demand the processing of his personal data. To the extent applicable, the Sub-processor shall assist the Data Processor in connection with the Data Controller's protection of data subjects' right to data portability and the right to oppose automatic decisions, including profiling.
	3. The Sub-processor is liable to the data subject if errors or negligence of Sub-processor incurs the recorded financial or non-financial losses due to their rights or privacy being violated.

**5 Information Security**

1. Sub-processor shall ensure appropriate technical, physical and organisational security measures to protect personal data covered by this Agreement against unauthorised or unlawful access, alteration, deletion, damage, loss or inaccessibility as detailed in Schedule F (Security Policy)
2. Sub-processor shall provide sufficient information and training to their own employees in order to safeguard the security of personal data processed on behalf of the Data Processor.
3. Sub-processor must document the training of their own employees in information security. The documentation should be available to the Data Processor.

**6 Confidentiality Obligations**

1. Only employees of Sub-processor who have a service need for access to personal data managed on behalf of a Data Processor can be granted such access. The Sub-processor is required to document access control policies and procedures. The documentation should be available to the Data Processor.
	1. Sub-processors shall ensure that employees of Sub-processors are subject to a duty of confidentiality regarding documentation and personal data that they may have access to in accordance with this Agreement. This provision also applies after termination of the agreement.

**7 Access to Documentation**

* 1. The Sub-processor is obliged to provide the Data Processor with access to all documentation that is necessary for the Data Processor to assist Data Controller to fulfill his/her duties under the current GDPR legislation.
	2. Sub-processor is obliged to provide the Data Processor with access to other relevant documentation that enables the Data Processor to assess whether the Sub-processor complies with the terms of this Agreement.
	3. The Data Processor may provide the Data Controller with access to the documentation to enable the controller to fulfill his/her obligations under the applicable data protection legislation, but also has a duty of confidentiality with regard to confidential documentation that the Sub-processor makes available to the Data Processor.

**8 Duty to Notify in Case of Security Breach**

* 1. Sub-processor shall notify the Data Processor without undue delay if personal data processed on behalf of the Data Processor is exposed to security breaches which entail a risk of violations of the data subjects' privacy.

8.2 The notification to the Data Processor shall include, as a minimum, information describing the breach, which data subjects are affected by the breach, what personal information is affected by the breach, what immediate action has been taken to deal with the breach, and any preventive measures that may have been taken to avoid it similar events in the future.

8.3 The Data Processor is responsible for ensuring that notifications of security breaches from the Sub-processor are passed on to the Data Controller.

**9 Subcontractors**

* 1. Sub-processor is obliged to enter into separate agreements with any subcontractors that regulate the subcontractor's processing of personal data on behalf of Sub-processor.
	2. In agreements between Sub-processor and subcontractors, subcontractors shall be required to fulfill all obligations that the Sub-processor itself is subject to under this Agreement. The Sub-processor is required to submit the agreements to Data processor on request. The Data Processor may submit the agreements to the Data Controller.
	3. Sub-processor shall verify that all subcontractors comply with their contractual obligations, that information security is satisfactory and that subcontractor employees are aware of their obligations and fulfill them.
	4. Data Processor approves that the Sub-processor engages the subcontractors listed in Annex II to this Agreement.
	5. Sub-processor cannot engage subcontractors other than those listed in Annex II without prior approval of the Data Processor. In the event of such a change, an amendment document must be attached as an annex to this Agreement, dated and signed by both parties.
	6. Sub-processor is liable for damages in accordance with Clause 14 for financial losses of the Data Processor due to illegal or unlawful processing of personal data or insufficient information security of subcontractors.

**10 Transfer to Countries Outside the EU/EEA**

* 1. Personal data processed by a Sub-processor on behalf of a data processor may be transferred to countries outside the EU / EEA (third countries). Such transfer may occur under certain conditions. The rules on transfer to third countries can be found in Articles 45-47 and 49 of the EU's Privacy Regulation.
	2. The rules also apply to backup and other transfer of personal data that occurs in connection with the administration of the service in question. These rules mean, among other things, that the transfer will be legal if it happens to an EU-approved third country ‘Adequacy Decision’, and in the individual States within the United States that have been granted the ‘Adequacy Decision’ for the type of information provided in that particular company's affiliation, or on the basis of EU standard contracts for the transfer of personal data to third-country data processors (EU's "Standard Contractual Clauses").

*<<Note: Use of the latter requires the agreement to be entered into directly between the controller and the Sub-processor, which is arranged by a contracting authority from the Data Controller to the Data Processor. >>*

**11 Security Audits and Impact Assessments**

* 1. Sub-processors shall regularly carry out security audits of their own work to secure personal data against unauthorised or illegal access, alteration, deletion, damage, loss or unavailability.
	2. Sub-processors will conduct security audits of the information security in the business. Security audits shall include the Sub-processor's security objectives and security strategy, security organization, guidelines, and procedures for security work, established technical, physical and organisational security measures and work on information security with subcontractors. It shall also include procedures for alerting Data Processor in case of security breaches and routines for testing contingency and continuity plans.
	3. Sub-processors must document the security audits. The Data Processor shall be given access to the audit reports. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the current Maltese personal data legislation.
	4. If an independent third party conducts security audits for the Sub-processor, the Data Processor shall be informed of which auditor is used and have access to summaries of the audit reports.
	5. The Data Processor can provide the Data Controller with access to summaries of the audit reports for the Data Controller to fulfill his/her duties according to current Maltese personal data legislation.
	6. Sub-processors shall, at the request of the Data Processor, assist the Data Processor if the use of the service means that the Data Controller has an obligation to assess the consequences of privacy, cf. Regulation (EU) 2016/679, Articles 35 and 36.

**12. Return and Deletion**

* 1. Upon termination of this Agreement, the Sub-processor is obliged to delete and/or return all personal data processed by the Sub-processor on behalf of the Data Processor in connection with the Main Agreement. The Data Processor decides how the return of personal data should take place, including the format to be used.
	2. Sub-processors shall delete personal data from all storage media containing personal data processed by the Sub-processor on behalf of the Data Processor. Deletion must occur by Sub-processor using a deletion tool approved by the Data Processor or by overwriting. This also applies to backups of personal data.
	3. Sub-processors shall document that deletion of personal data has been carried out in accordance with this Agreement. The documentation shall be made available to the Data Processor. The Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the data protection legislation and regimes.
	4. On termination of the main Contract for any reason or expiry of the Term:

(a ) the Sub- processor shall as soon as reasonably practicable return (as directed in writing by Data Controller or Data Processor) all Personal Data. The Sub-processor shall use reasonable commercial efforts to fulfil such request within ten working days (10) days of its receipt; or

( b) if the Data Controller elects for destruction rather than return of the materials the Sub-processor shall ensure that all Personal Data is immediately deleted from the Data Processor System.

* 1. The Sub-processor shall provide written confirmation (in the form of a signed letter) no later than fourteen (14) days after termination or expiry of or expiry of this Agreement of compliance with Clause 12.4.

**13 Breach**

* 1. In the event of any material breach of the terms of this Agreement due to errors or negligence on the part of the Sub-processor, the Data Processor may terminate the Agreement with immediate effect. Sub-processors will continue to be obliged to return and/or delete personal data processed on behalf of the Data Processor in accordance with the provisions of clause 12 above.
1. **Compensation**

14.1 The Data Processor may claim compensation for financial losses for errors or neglect on the part of the Sub-processor, including breach of the terms of this agreement.

1. **The Data Protection Agreements Duration**

15.1 This Agreement applies as long as the Sub-processor processes personal data on behalf of Data Processor originating in the Main Contract Service agreement.

Annex A: Purposes for which the Data Processor may process Personal Data *Social Security System*

|  |  |
| --- | --- |
| **Description** | **Details** |
| Subject matter of the processing | Contractor is to provide the Services as detailed in this Contract in relation to the Social Security.  |
| Duration of the processing  | Throughout the Term of the Contract.  |
| Nature and purposes of the processing | The purpose of this contract is to modernise the core Social Security system. During the execution of this contract, the current system, its functionality and code business logic will be technically analysed, and new modernised products and components will be developed, tested and implemented.To provide the Services as detailed in the Contract.  The contractor is required to access Social Security system authorized environments and databases. Primary access shall be granted to authorized environment and database which holds sanitized data. The data processing involves using sanitised real-life cases (on the authorized environment) to analyze current functionality, develop and test modernized modules and functionality, and to complete testing activities during the term of the contract.All the necessary technical measures have been taken to sanitise the data. However, there may be exceptional instances during this contract term, where test data (which is a replica of the SABS production database) may be accessed to understand specific scenarios and to perform functional simulation runs and/or tests.The Data Controller shall approve the access to and processing of test data when exceptional instances emerge while completing the assigned tasks throughout the contract term.  |
| Type of Personal Data | Standard personal data includes name, surname, id card number, social security number, pension number, date of birth, date of death, address, contact details, civil status.Sensitive personal data includes gender, relations, ended relations, medical conditions (high level description only), disability conditions, invalidity conditions, citizenship, residency, subsidiary protection, income details, income status, social assistance entitlements, financial income and means. |
| Categories of Data Subject | The system has a database that stores all Maltese citizens, including foreigners with interactions with the Social Security. Categories include subjects from all strata of society but there is no categorisation in the system. All subjects in the system are treated as Social Security Beneficiaries, which could be pensioners, sick or invalid persons, unemployed persons, social cases, etc. Data Subjects can only be categorised under a specific heading according to the benefits received.  |
| Plan for return and destruction of the data once the processing is complete  | No data is to be copied or extracted and stored by the Contractor.Extracts of any instances of samples of sanitised live data will be destroyed as soon as they are no longer required. |

Annex A: Purposes for which the Data Processor may process Personal Data *Taxation System*

|  |  |
| --- | --- |
| Description | Details |
| Subject matter of the processing  | Contractor is to provide the Services as detailed in this Contract in relation to Taxation.  |
| Duration of the processing  | Throughout the Term of the Contract.  |
| Nature and purposes of the processing | The purpose of this contract is to modernise the core Taxation system. During the execution of this contract, the current system will be technically analysed, and new modernised components will be developed and implemented.All the necessary technical measures have been taken to sanitise the data, however there may be exceptional instances during this project where live data may be accessed to understand specific scenarios and to perform simulation runs. |
| Type of Personal Data | Standard personal data includes name, surname, ID card number, Social Security Number, Date of Birth, Date of Death, mailing address, contact details, and civil status.Sensitive personal data includes gender, relations, ended relations, citizenship, financial and tax details |
| Categories of Data Subject | The taxation system contains information required related to the administration of various tax legislations including the Income Tax Act, Income Tax Management Act, the Capital Transfer Duty Act, VAT and ECO Acts. It contains information on natural Maltese nationals and foreign persons. All subjects in the system are categorised as taxpayers. Taxpayers can be employees, self-employed, employers, self-occupied, pensioners, students, and foreign persons registered under special tax scheme. |
| Plan for return and destruction of the data once the processing is complete  | No data is to be copied or extracted and stored by the Contractor. Extracts of any instances of samples of sanitised live data will be destroyed as soon as they are no longer required. |

**ANNEX B – List of Authorised Sub-Contractor/s**

The parties have agreed that the following sub-contractors may be used by the respective parties under the Agreement:

Sub-processors sub-contractors *(if any):*

*[Specification of authorised subcontractors.]*

1. MITA’s working hours span from 0730/0830hours to 1630/1730hours local time. (Malta operates within Central European Time (CET) / Central European Summer Time (CEST) Time zone (Local Time) and is 1 hour ahead of Coordinated Universal Time (UTC)). [↑](#footnote-ref-1)
2. Work assigned may include a combination of modernisation-related work and legacy-related work (legacy-related work will make up a smaller percentage of the overall work assigned). [↑](#footnote-ref-2)
3. A free, open-source Unit Testing Framework for .NET. [↑](#footnote-ref-3)
4. AutoFixture is an open-source library for .NET designed to minimize the ‘Arrange’ phase of the unit tests to maximise maintainability. Its primary goal is to allow developers to focus on what is being tested rather than how to setup the test scenario, by making it easier to create test data. [↑](#footnote-ref-4)
5. Fluent assertions is a set of .NET extension methods that allow you to specify the expected outcome of a TDD-style unit test more naturally. [↑](#footnote-ref-5)