AGREEMENT BETWEEN DATA PROCESSOR AND SUB-PROCESSOR ON THE PROCESSING PERSONAL DATA

(SUB-PROCESSOR AGREEMENT)

BETWEEN Malta Information Technology Agency and whose registered address is at Gattard House, National Road, Blatal-Bajda HMR 9010 (hereinafter referred to as the "Data Processor");

AND [name of sub-processor] having its offices at [address of sub-processor] (hereinafter referred to as the "Data Sub-Processor");

Preambles

(a) 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 the Contract – Service Contract [Contract number].
.

(b) 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 I and Annex II (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.

2. Purpose of the Agreement

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").

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 *[name of project]* in accordance with agreement between the parties entered into *[date]* ("Main Service Contract Agreement").

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.

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.

It must be stated in Annex III 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 8.

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 1 and Annex II of the 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.

3. Processing

Sub-processors shall follow the written and documented instructions for the processing of personal data that the Data Processor has decided to apply.

Sub-data processors undertake to comply with all obligations in accordance with the applicable personal data legislation applicable to the processing of personal data.

Sub-processor undertakes to notify Data Processor if Sub-processor receives instructions from Data Processor that violates the privacy regulations.

4. The Rights of Data Subjects

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

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Data Protection Commissioner or any other regulatory / supervisory authority in connection with this Schedule; and
(e) 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.

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.

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.

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

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.

Sub-processor must document their own security organisation, guidelines and procedures for security work, risk assessments and established technical, physical or organisational security measures. The documentation should be available to the data processor. Data Processor can provide the Data Controller with access to the documentation so that the Data Controller can fulfill his/her duties under the personal data legislations.

Sub-processor will establish continuity and contingency plans for effective management of serious security incidents. The documentation should be 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 legislations and regimes.

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.

Sub-processor must document the training of their own employees in information security. The documentation should be 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 current personal data legislations.

6. Confidentiality

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.

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

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.

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.

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

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.

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.

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

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.

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.

Sub-processor shall verify that all subcontractors comply with their contractual obligations, in particular that information security is satisfactory and that subcontractor employees are aware of their obligations and fulfill them.

Data Processor approves that the Sub-processor engages the subcontractors listed in Annex III to this Agreement.

Sub-processor cannot engage subcontractors other than those listed in Annex III 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.

Sub-processor is liable for damages in accordance with Clause 13 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

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. The rules also apply to backup and other transfer of personal data that occurs in connection with the administration of the service in question, such as support. These rules mean, among other things, that the transfer will be legal if it happens to an EU-approved third country, 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").

11. Security audits and impact assessments

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.

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.

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.

If an independent third party conducts security audits at the Sub-processor, the Data Processor shall be informed of which auditor is used and have access to summaries of the audit reports. The Data Processor can provide the Data Controller with access to summaries of the audit reports in order for the Data Controller to fulfill his/her duties according to current Maltese personal data legislation.

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. Sub-processor can assist in the implementation of privacy-promoting measures if the impact assessment shows that this is necessary.

12. Return and deletion

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.

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.

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.

On any 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.

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 the Contract.

13. Breach

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 clause11 above.

14. Compensation

The Data Processor may claim compensation for financial losses that errors or neglect on the part of the Sub-processor, including breach of the terms of this agreement, have caused the Data Processor, cf. also paragraphs 3 and 8 above.

Sub-processor is liable for direct financial loss, including administrative infringement fees and claims that are addressed to the Data Processor, which can be reversed in violation of the Sub-processor's obligations under this agreement.

15. The Data Protection Agreements duration

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

Authorised Signature	Authorised Signature
Name and Position	Name and Position
Date	Date
Data Processor	Data Sub-Processor

ANNEX 1 – Purposes for which the Data Processor may process Personal Data (Social Security System)

Description	Details
Subject matter of the processing (i.e. why the data is being processed/purpose of the Contract)	Contractor is to provide the Services as detailed in this Contract in relation to the Social Security.
Duration of the processing (e.g. throughout the Contract or until a particular phase is reached)	Throughout the Term of the Contract.
Nature and purposes of the processing (i.e. why is it lawful to process such data: six lawful basis for processing (Consent/Contract/Legal Obligation/Vital Interests/Public Task/Legitimate Interest). What is important is that this processing is necessary. If special category of data – you need to identify the general purposes for lawful processing as well as the special purpose for such processing). Same applies if we are processing criminal convictions – we need a specific reason.	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 Personal Data is broadly defined as data from which a living individual can be identified or identifiable (by anyone), whether directly or indirectly, by all means reasonably liked to be used including names, location data and online identifiers. Special Categories of personal data (special measures have to be taken with Sensitive Data): racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, genetic data or biometric 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 A Data subject is a natural person whose personal data is processed. Categories may include: patients/employees/students/users etc.	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(please refer to article 9).	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 II: 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 III – List of authorised Subcontractors

The parties have agreed that the following subcontractors may be used by the respective parties under the Agreement:

Subcontractors:

[Specification of any authorised subcontractors.]