DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") is entered into between

THE ENERGY & WATER AGENCY, as established by L.N. 50 of 2014, ("**the Agency**"), herein also referred to as the "**Data Controller**",

And

[CONTRACTOR]

and is an addendum to, and should be construed in conjunction with, the contract entered into by the same Parties for [DESCRIPTION OF TENDER] (the "**Principal Agreement**").

Preambles

WHEREAS

(A) The Parties have entered into an Agreement (the Principal Agreement) by virtue of which [CONTRACTOR], (the Data Processor), shall be processing data on behalf of the Agency in fulfilment of contractual obligations.

(B) The Agency is the Data Controller of any Personal Data processed by [CONTRACTOR], including Personal Data collected, recorded, organised, stored, altered, retrieved, used, disclosed by transmission, disseminated or otherwise made available, erased or destroyed, whether or not by automated means, in fulfilment of the obligations arising under the Principal Agreement.

(C) The Personal Data shall be exclusively processed in fulfilment of the Data Processor's obligations under the Principal Agreement.

(D) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework set out in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") and of Chapter 586 of the Laws of Malta (the Data Protection Act 2018).

(E) The Parties wish to lay down their reciprocal rights and obligations regulating the processing of Personal Data.

1 Definitions

'Business Purpose/ Purpose' means the purpose/s specified in Annex A.

'Confidential Information' means such data as defined in Clause 6 of this Agreement.

'Data Controller / Controller' shall have the same meaning of 'controller' as set out in the GDPR, and for the purposes of this Agreement shall be the Energy and Water Agency.

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

'Data Processor / Processor' shall have the same meaning of 'processor' as set out in

the GDPR, and for the purposes of this Agreement shall be [CONTRACTOR]

'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 Protection Legislation' means the Data Protection Act 2018 (Cap 586) and the General Data Protection Regulation (EU) 2016/679 (GDPR), 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 Subject' shall have the same meaning of 'data subject' as set out in the GDPR.

'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.

'EEA' means the European Economic Area.

'Principal Agreement' means the service contract entered into for the purposes of [INSERT DESCRIPTION] (Tender Ref No #####).

'Personal Data' shall be interpreted according to the meaning set out in the GDPR and shall mean any Personal Data which is processed by the Data Processor on behalf of the Agency pursuant to or in connection with the Principal Agreement, and shall be construed to include any additional Personal Data which the Contracted Data Processor acquires and retains in the course of fulfilling its obligations under the Principal Agreement.

'Personal Data Breach' shall have the same meaning as set out in the GDPR.

'Process' shall have the same meaning of 'processing' as set out in the GDPR.

'Protective Measures' means the measures to be taken by the Data Processor in line with Article 32 of the GDPR 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 Data Processor to the Data Controller as detailed in the Principal Agreement

'Sub-Processor' means any third party appointed to process Personal Data on behalf of the Data Controller related to the Principal Agreement.

2 Scope

2.1 The Parties agree that the terms and conditions set forth in this Agreement shall regulate the processing by the Data Processor of Personal Data controlled by the Data Controller.

3 Data Protection Obligations

Processing

3.1 The Data Controller hereby authorises the Data Processor to process Personal Data only to the extent, and in such a manner, as is necessary for the Business Purpose and in accordance with the instructions as detailed in Annex A and subject to the security measures as detailed in Annex B. The Parties will ensure that any amendments to Annex A and the security measures are to be carried out in writing through an amendment to this Agreement that is to be annexed to this document. The Data Processor shall not process Personal Data for any other purpose or without any specific written instructions from the Data Controller.

3.2 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction of the Data Controller infringes the Data Protection Legislation.

Access to Personal Data

3.3 The Data Processor shall ensure that access to the Personal Data is limited to:

(a) those employees who need access to the Personal Data for the Purpose identified in Annex A; and

(b) provided that such employee is granted access only to such part or parts of the Personal Data that is strictly necessary for performance of that employee's duties.

3.4 The Data Processor shall ensure that all its employees, sub-processor and its personnel (if any) shall observe unconditional confidentiality as regards the Processing of Personal Data. More specifically the Data processor shall ensure that they:

(a) are informed of the confidential nature of the Personal Data;

(b) have undertaken training in the laws relating to the handling of Personal Data; and

(c) are aware both of the Data Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

3.5 The Data Processor shall take reasonable steps to ensure the reliability of any of its employees who have access to Personal Data.

3.6 Where the Data Controller is not satisfied with the performance of the Data Processor's personnel providing the Service, the Data Controller shall immediately notify the Data Processor in writing giving reasons for its dissatisfaction, and the Data Processor shall use its best endeavours to rectify the situation. For the purposes of this Clause the performance of the employee shall be deemed unsatisfactory, *inter alia*, where: (i) such employee is incompetent; (ii) such employee is negligent in the performance of his duties; (iii) employee lacks the skills and experience required; or (iii) his behaviour at the place of work is unacceptable or unsuitable.

Retention Period

3.7 Retention periods for all categories of Personal Data processed are to be established by the Data Controller and adhered to by the Processor, keeping in mind Data Protection principles relating to storage limitation. As per the Regulation, such retention periods will not apply to statistical or anonymised data.

Data Protection Impact Assessment

3.8 The Data Processor shall, as requested by the Controller, provide all reasonable assistance to the Data Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Data processor and after taking into account the nature of the processing and the information available to the processor, include: (a) a systematic description of the envisaged processing operations and the purpose of the processing; (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services; (c) an assessment of the risks to the rights and freedoms of Data Subjects; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

Data loss Event and Personal Data Breaches

3.9 The Data Processor shall immediately inform the Data Controller of any Data Loss Event, Personal Data Breach(es) and/or if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable in the course of providing the Services in accordance with this Agreement.

3.10 The Data Processor as soon as reasonably practicable, must provide the Controller with the full details (using such reporting mechanism as specified by the Controller from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

Transfer of Data outside the EU/EEA

3.11 The Data Processor shall not transfer Personal Data outside the EU/EEA unless the prior written approval of the Data Controller is obtained.

Data Subject Requests and other requests

3.12 The Data Processor shall notify the Data Controller 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 Agreement; 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 Data Processor's obligation of notification as detailed in this Clause shall include the provision of further information to the Data Controller in phases, as details become available.

3.13 The Data Processor shall provide the Data Controller with full assistance including by promptly providing:

(i) details and copies of the complaint, communication or request;
(ii) such assistance as is reasonably requested by the Controller to enable the Controller to comply with Data Subject rights such as requests for access, rectification, and erasure, and other requests such as complaints or communication made by the Data Subjects, within the relevant timescales set out in the Data Protection Legislation;
(iii) the Data Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
(iv) assistance as requested by the Controller following any Data Loss Event;

(v) assistance as requested by the Controller with respect to any request from the supervisory authorities.

Assistance and Collaboration

3.14 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Controller's and Data Processor's obligations laid down in the GDPR. The Data Processor shall ensure that it co-operates with any supervisory authority as necessary.

4. **Warranty**

4.1 Each party warrants to the other that it will process the Personal Data in compliance with the Data Protection Legislation and all applicable laws, enactments, regulations, orders, standards and other similar instruments.

4.2 The Parties agree to hold each other harmless against any action taken against either party by any third party for a default imputable to the other party.

5 Security and Auditing

5.1 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations as detailed in Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Data Processor.

5.2 The Data Processor warrants that, having regard to the state of technological development and the cost of implementing any measures, it will take Protective Measures against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of or damage to Personal Data to ensure a level of security appropriate to:

(a) the risk of and/or the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
(b) the nature of the data to be protected including, but not limited to, the security measures set out in Annex B.

5.3 The Data Processor shall create and maintain complete and accurate records as detailed in Article 30 of the GDPR.

5.4 The Data Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

6 Confidentiality Obligations

6.1 The Data Processor acknowledges that the Personal Data is Confidential Information.

6.2 The Data Processor shall not:

(a) make copies of the Personal Data, unless approved in writing by the Data Controller, provided that the copies of the Personal Data which are required for the carrying out of the processing as described in Annex A2 shall be deemed to be pre-authorised for the purposes of this Clause;

(b) extract, re-utilise, use, exploit, redistribute, re-disseminate, copy or store the Personal Data other than for the Business Purpose; or

(c) disclose any Confidential Information in whole or in part to any third party, except as expressly permitted by this Clause.

6.3 The Data Processor may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, as far as it is legally permitted to do so, it gives the Controller as much notice of the disclosure as possible.

6.4 The Data Controller reserves all rights in its Confidential Information. No rights or obligations in respect of Confidential Information, other than those expressly stated in the Principal Agreement and this Agreement, are granted to the other party, or are to be implied from the Principal Agreement and this Agreement.

6.5 The provisions of this Clause shall continue to apply after termination of the Principal Agreement.

7 Indemnity

7.1 Each Party agrees to indemnify and keep indemnified and defend at its own expense the other Party against all costs, claims, damages or expenses incurred by the other Party or for which the other Party may become liable due to any failure by the first Party or its employees or agents to comply with any of its obligations under the Principal Agreement or this Agreement.

8 Appointment of Sub-processors

8.1 The Data Processor shall not employ any Sub-processors to assist it in the data processing activities as detailed in this document unless it has the prior written agreement of the Data Controller.

8.2 In the event of the appointment of a Sub-processor, the Agency reserves the right to establish *ad hoc* terms for the Processing of Personal Data by the Sub-processor, which sub-processing shall be governed by an Agreement between the Processor and Sub-Processor which shall be on terms which are substantially the same as those set out in this Agreement and in line with the instructions laid down in Annex A.

8.3 If the Data Controller agrees to such Sub-processors, the Data Processor shall ensure that any Sub-processor's agreement shall be:

(a) on terms which are substantially the same as those set out in this Agreement; and

(b) terminated automatically on termination, for any reason, of the Principal Agreement.

Notwithstanding the approval granted by the Data Controller, the initial processor shall remain fully liable to the Data Controller for the performance of its sub-processor's obligations.

9 Term and Termination

9.1. This Agreement and the Data Processor's right to retain and Process the Agency Personal Data according to the provisions of this Agreement shall immediately terminate in the event that the Agency, for any reason, no longer remains a Data Controller of said Data.

9.2. Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination of the Principal Agreement shall remain in full force and effect.

9.3. Termination of the Principal Agreement or this Data Processing Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at termination.

9.4. On any termination of the main Principal Agreement or this Agreement for any reason or expiry of the Term:

(a) the Data Processor shall as soon as reasonably practicable, as directed in writing by Data Controller, destroy all of the Data Controller's Personal Data or relinquish or transfer access thereto in favour of the Data Controller. The Data 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, the Data Processor shall ensure that all Personal Data is immediately deleted from the Data Processor System.

9.5. The Data 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/this Agreement of compliance with Clause 9.4.

9.6. This Agreement is entered into with effect from the date last set out below.

[SIGNATURES]

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

Description	Details
Business Purpose	
Duration of the processing	
Legal Basis for Processing	
Type of Personal Data	
Categories of Data Subject	
Nature of Processing	
Retention and Destruction of Shared Data	

Annex A1: Energy and Water Agency's Legal Basis for the Processing of the Personal Data (General)

[The legal basis for the processing of the data to be included]

Annex A2: Processing

[A description of the processing to be included – Project Specific]

Annex B: Security Requirements

[This list may be amended, subject to the requirements and context of the specific contract and the processing involved]

The Data Processor shall be responsible for:

- Safeguarding the confidentiality, the integrity, and the availability of the Personal Data which is the subject of this Data Processing Agreement.
- Reviewing periodically and keeping updated all security requirements indicated in this Annex.
- Ensuring that physical controls are in place to prevent unauthorised access to the Processor's premises.
- Ensuring that any changes that occur to the processing are carried out through planning, testing and an assessment.
- Ensuring that secure disposal is affected.
- Monitoring of back-ups, capacity and performance on a regular basis.
- Setting-up necessary controls against malicious codes.
- Ensuring that the Controller's Personal Data in their possession is stored in a secure manner and physically protected from unauthorised access and damage.
- Ensuring that all personal computers and data storage devices are password protected to prevent unauthorised access.
- Ensuring that the papers and storage media containing Controller 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 Controller Data.
- Ensuring that in cases where work is carried out outside the premises, appropriate security measures are implemented.
- Providing accurate information in a timely manner in the case of an investigation or security breach.

Annex C- List of Approved Sub- Processors –

Name of the Sub-Processor	Registered Business Address	Actual Location of Processing