

## Data Processing Agreement

The Land Development Agency

AND

**[ Insert Name Here ]**

**THIS AGREEMENT** is made on **[ PLEASE INSERT DATE ]**

### BETWEEN:

1. **The Land Development Agency (“LDA”)**, with its address at George's Court, 54-62 Townsend St, Dublin 2, D02 R156, acting in its capacity as Data Controller (the “**Data Controller**”)
2. **[Processor Name]**, a company registered in Ireland with company number **XXXX** whose registered address is **[Organisation Address]** (the “**Data Processor**”); and

(each a “**Party**” and collectively the “**Parties**”).

## BACKGROUND:

The Data Controller and the Data Processor are parties to a customer Services Agreement dated [ **Insert Date Here** ] the "Service Agreement" pursuant to which the Data Processor provides [ **Insert description of the services** ] to the Data Controller.

In connection with the provision of the Services, the Data Processor may process Personal Data on behalf of the Data Controller. This Data Processing Agreement sets out the terms and conditions governing such processing and is intended to ensure that the Parties comply with the applicable Data Protection Laws and, in particular, Article 28 of the General Data Protection Regulation (GDPR).

## DEFINITIONS AND INTERPRETATION:

For the purposes of this Agreement, unless the context otherwise requires, the following terms shall have the following meanings:

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>“Data Protection Laws”</b>               | means all applicable laws and regulations relating to the processing of Personal Data and privacy including the Irish Data Protection Act 2018, the General Data Protection Regulation 2016/679 (the “GDPR”) and the European Communities (Electronic Communications, Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011) and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted or consolidated; |
| <b>“Effective Date”</b>                     | means the date of this Agreement;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>“General Data Protection Regulation”</b> | means Regulation (EU) 2016/679, known as the General Data Protection Regulation (the “ <b>GDPR</b> ”);                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>“Data Controller”</b>                    | means the entity which, alone or jointly with others, determines the purposes and means of the processing of the Personal Data;                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>“Data Processor”</b>                     | means the entity which processes Personal Data on behalf of the Data Controller;                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**“Law”**

means any constitution, law, treaty, statute, ordinance, code, rule, regulation, executive order, administrative order or other order, judgment or determination of any Governmental Authority, Regulatory Requirement, applicable principle of common or civil law, or any binding agreement with any Governmental Authority, as amended from time to time within the scope of this Agreement;

**“Personal Data”**

has the meaning as set out in Data Protection Laws.

**Services**

means the services provided by the Data Processor to the Data Controller pursuant to the Services Agreement

**“Services Agreement”**

means the agreement, contract, purchase order, service level agreement or other written arrangement entered into between the Data Controller and the Data Processor pursuant to which the Data Processor provides services to the Data Controller, as amended, varied or replaced from time to time; and

**“Special Categories of Data”**

has the meaning as set out in Data Protection Laws.

.

This Agreement, including these definitions and its recitals and schedules, is a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the data processing (as well as the Personal Data covered) are specified in Schedule 1 hereto.

**WHEREAS:**

Under the GDPR, a written Data Processing Agreement must be in place between the Data Controller and any organisation which processes personal data on its behalf, governing the processing of the data. This Agreement is intended to satisfy that obligation.

**TERMS**

The parties agree that:

- 1.1 The Data Controller and the Data Processor acknowledge that for the purposes of the Data Protection Laws (as amended), the Land Development Agency is the Data Controller and **[ Insert Name Here ]** is the Data Processor in respect of any Personal Data.
- 1.2 The Data Processor shall process Personal Data only to the extent necessary to provide the **Services** and perform its obligations under the **Services Agreement**.
- 1.3 The Data Controller shall instruct the Data Processor to process the Personal Data in any manner that may reasonably be required in order for the Data Processor to carry out the processing in compliance with this Agreement and in compliance with Applicable Data Protection law.
- 1.4 The Data Controller shall not issue instructions that would require the Data Processor to act in breach of the Data Protection Laws. Where the Data Processor considers that an instruction infringes the Data Protection Laws, it shall notify the Data Controller without undue delay and shall not be obliged to comply with such instruction until the matter has been resolved..
- 1.5 The details of the transfer and of the Personal Data are specified in Schedule 1. The parties agree that Schedule 1 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required by law. The parties may execute additional annexes/schedules to cover additional transfers, or may include multiple transfers in Schedule 1.
- 1.6 This Agreement shall continue for no less a term than the term of the Services Agreement.
- 1.7 The rights and obligations of the parties with respect to each other under this Clause 1 shall survive any termination of the Agreement.

## **2. REGULATORY COMPLIANCE**

- 2.1 To the extent required by law or regulation:
  - 2.1.1 The Data Processor shall cooperate with the in connection with any activities performed by the Data Processor;
  - 2.1.2 The Data Controller, its auditors and any competent Supervisory Authority shall have effective access to data related to such activities, as well as effective access to the Data Processor's business premises;
  - 2.1.3 Nothing in this Agreement shall prevent a competent Supervisory Authority from exercising any statutory powers of inspection or investigation conferred upon it under the Data Protection Laws; and

2.1.4 The Data Processor shall give prompt notice, and in any event within **24 hours**, to the Data Controller of any development that may have a material impact on the Data Processor's ability to perform services effectively under this Agreement and in compliance with applicable laws and regulatory requirements.

### **3. OBLIGATIONS OF THE DATA CONTROLLER**

The Data Controller warrants and undertakes that:

- 3.1 The Personal Data has been collected, processed, and disclosed to the Data Processor in accordance with the Data Protection Laws.
- 3.2 It has used reasonable efforts to determine that the Data Processor is able to satisfy its legal obligations under this Agreement.
- 3.3 It will respond to enquiries from Data Subjects and the Data Protection Commission or other supervisory authority where appropriate concerning processing of the Personal Data by the Data Controller, unless the parties have agreed that the Data Processor will so respond, in which case the Data Controller will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Processor is unwilling or unable to respond. Responses will be made within a reasonable time and in accordance with the applicable Data Protection laws.
- 3.4 It will make available, upon request, a copy of this Agreement to Data Subjects who are relevant to the processing, the subject matter of this Agreement, unless this Agreement contains confidential information, in which case it may redact such information. The Data Controller shall abide by a decision of the Data Protection Commission or other supervisory authority where appropriate regarding access to the full text of this Agreement by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Controller shall also provide a copy of this Agreement to the Data Protection Commission or other supervisory authority where appropriate where required.

### **4. OBLIGATIONS OF THE DATA PROCESSOR**

The Data Processor warrants and undertakes that:

- 4.1 The Data Processor shall ensure that its internal operating systems only permit properly authorised personnel to access Personal Data.
- 4.2 The Data Processor shall provide appropriate training to its personnel with respect to:
  - (i) the correct handling of Personal Data so as to minimise the risk of security breaches; and
  - (ii) the requirements of the applicable Data Protection Laws.
- 4.3 The Data Processor acknowledges and agrees that it will:

- (i) only Process Personal Data in accordance with the Data Controller's written instructions, including with regard to transfers of personal data to a Third Country or an international organisation (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by the Data Controller to the Data Processor from time to time, and the Data Controller shall ensure it gives only lawful written instructions);
- (ii) only use, reproduce or otherwise Process any Personal Data collected in connection with providing the Services, to the extent necessary to provide the Services;
- (iii) not modify, amend or alter the contents of the Personal Data, except as directed by the Data Controller;
- (iv) not, without the Data Controller's written approval, Process any Personal Data on any Data Processor systems on which data (including any Personal Data) is Processed for any person outside of the Data Controller; and
- (v) implement and maintain a system for logging and identifying all Data Processor personnel accessing any Personal Data through Data Processor systems and if requested by the Data Controller, the Data Processor shall provide to the Data Controller a copy of the access log.

4.4 The Data Processor shall implement appropriate technical and organisational measures (in particular those required under the GDPR and the Data Protection Acts) to assure a level of security appropriate to the risk to the security of Personal Data, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data in accordance with the Data Processor's obligations under Data Protection Laws and Schedule 2 of this Agreement (the "**Technical, Organisational and Security Measures**"). The Security Measures may also include as appropriate:

- (i) the pseudonymisation and encryption of Personal Data;
- (ii) the ability to ensure the ongoing confidentiality, integrity and availability of the Personal Data and resilience of the Data Processor systems used for such Processing;
- (iii) the ability to restore the availability and access to the Personal Data, in a timely manner but no later than forty eight (48) hours, in the event of a physical or technical incident; and
- (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.5 The Data Controller may notify the Data Processor immediately in the event that it does not consider that the Security Measures ensure an appropriate level of security for Personal Data and the Data Controller shall notify the Data Processor of any additional or amended security controls or measures which the Data Controller considers, in its reasonable opinion, is necessary to ensure compliance with Data Protection Laws. The Data Processor agrees to implement such additional security controls or measures.

- 4.6 The Data Processor agrees and warrants that the Security Measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected, having regard to the state of the art and the cost of their implementation.
- 4.7 Without limiting the Data Processor's other obligations under this Clause 4.7, the Data Processor:
- (i) may disclose Personal Data to its personnel but only those who:
    - a) need to know for the purpose of providing the Services (and only to that extent);
    - b) have been trained in accordance with Clause 4.2;
    - c) are subject to a binding contract to keep the Personal Data confidential (or are under an appropriate statutory obligation of confidentiality), and
  - (ii) may only disclose Personal Data to any other person with the prior written consent of the Data Controller, and, where the Data Controller provides its consent, only where the person is subject to a binding commitment to keep the Personal Data confidential (or are under an appropriate statutory obligation of confidentiality).
- 4.8 If the Data Processor or Data Processor personnel are required by Law and/or an order of any court or competent jurisdiction or any regulatory, judicial or governmental body to disclose the Personal Data, the Data Processor shall, except where prohibited by Law, first:
- (i) give the Data Controller notice of the details of the proposed disclosure;
  - (ii) give the Data Controller a reasonable opportunity to take any steps it considers necessary to protect the confidentiality of the Personal Data, including but not limited to, seeking such judicial redress as the Data Controller may see fit in the circumstances;
  - (iii) give any assistance reasonably required by the Data Controller to protect the confidentiality of the Personal Data; and
  - (iv) inform the proposed disclosee that the information is confidential.
- 4.9 Without limiting the Data Processor's other obligations under this Agreement, the Data Processor shall not engage any third party processors to Process Personal Data without the prior written consent of the Data Controller. If the Data Processor engages any third party to Process any Personal Data, the Data Processor shall impose on such third party, by means of a written contract, the same data protection obligations as set out in this Agreement.
- 4.10 The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of any third party processors and shall not make any such changes without the prior written consent of the Data Controller.
- 4.11 The Data Processor shall remain liable to the Data Controller for Processing by such third parties as if the Processing was being conducted by the Data Processor.

- 4.12 The Data Processor acknowledges and agrees that the Data Processor or Data Processor personnel may not transfer Personal Data to any Third Country except to the extent that the transfer is expressly approved by the Data Controller in writing.

## 5. Assistance

- 5.1 Each Party shall co-operate with the other party to the extent necessary to enable that party to comply with any requests of the Data Protection Commission or other competent Supervisory Authority in respect of the Personal Data.

- 5.2 The Data Processor shall:

- (i) make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and the Data Protection Acts, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller;
- (ii) immediately inform the Data Controller if, in its opinion, an instruction given or request made pursuant to Clause 4.14 (i) infringes Data Protection Laws;
- (iii) taking into account the nature of the Processing, provide such cooperation and assistance, including by using appropriate technical and organisational measures, as the Data Controller may require for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR and in the relevant parts of the Data Protection Acts;
- (iv) provide such cooperation and assistance as the Data Controller may require to enable the Data Controller to comply with its obligations and in particular those obligations under Articles 32-36 of the GDPR and those obligations in the Data Protection Acts, including without limitation, to notify the Data Controller without undue delay and in any event within **twenty four (24)** hours following the Data Processor becoming aware of a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data ("**Personal Data Breach**"). The Data Controller shall without undue delay notify the Data Processor of any Personal Data Breach affecting the Data Processor;
- (v) immediately notify the Data Controller of any monitoring activities and measures undertaken by the Data Protection Authority that supervises the applicable Data Protection Laws;
- (vi) support the Data Controller regarding the Data Controller's obligations to provide information about the collection, processing or usage of Personal Data to a Data Subject;
- (vii) deal promptly and properly with all enquiries from the Data Controller relating to its Processing of the Personal Data and Special Categories of Personal Data;

- (viii) if the Data Processor receives any request by any person to access or correct Personal Data, the Data Processor shall, within two (2) Business Days, notify the Data Controller and provide the Data Controller with the full details of that request; and
- (ix) ensure that the Personal Data are not in any way used, manipulated, distributed, copied or processed for any other purpose than for the fulfilment of the contractual obligations, as explicitly agreed upon and arising from this Agreement.

## **6. RIGHT OF AUDIT**

- 6.1 The Data Processor shall maintain proper records of any Personal Data recovered from or on behalf of the Data Controller and of all training carried out with regard to the technical and organisational data Security Measures.
- 6.2 The Data Processor shall permit the Data Controller or its representatives to access all relevant systems (including the Data Processors systems), personnel, records and information of the Data Processor during normal working hours for the purpose of inspecting, testing and auditing the technical and organisational data Security Measures operated by the Data Processor and for the purpose of confirming the Data Processor's compliance with its obligations under this Agreement and with Data Protection Laws. The Data Processor shall promptly implement any reasonable requirement made by the Data Controller to improve the technical and organisational measures.

## **7. LIABILITY AND INDEMNITY**

- 7.1 The Data Processor will not be liable for any claim brought by a Data Subject arising from any action by the Data Processor to the extent that such action resulted directly from the Data Controller's instructions.
- 7.2 Except as provided for in Clause 7.1, the Data Processor shall indemnify the Data Controller for any monetary fine or penalty imposed on the Data Controller by the Data Protection Commission or other supervisory authority where appropriate that results from the Data Processor's breach of its obligations under this Agreement.
- 7.3 In the event that any claim is brought against the Data Controller by a Data Subject arising from any action by the Data Processor, to the extent that such action did not result directly from the Data Controller's instructions, the Data Processor shall indemnify and keep indemnified and defend at its own expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.
- 7.4 In the event that any claim is brought against the Data Processor by a Data Subject arising from any action or omission by the Data Processor to the extent that such action or omission resulted directly from the Data Controller's instructions, the Data Controller shall indemnify and keep indemnified and defend at its own expense the Data Processor against all costs, claims, damages or expenses

incurred by the Data Processor for which the Data Processor may become liable due to any failure by the Data Controller or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

## **8. TERMINATION**

8.1 In the event that either the Data Processor or the Data Controller is in breach of its obligations under this Agreement, then either the Data Processor or the Data Controller may temporarily suspend the processing of Personal Data to the Data Processor until the breach is repaired, or the Agreement is terminated.

8.2 In the event that:

8.2.1 the transfer of Personal Data to the Data Processor has been temporarily suspended by the Data Controller for longer than one month pursuant to paragraph 8.1;

8.2.2 compliance by the Data Controller with this Agreement would put it in breach of its legal or regulatory obligations in the country of import;

8.2.3 the Data Processor or Data Controller are in substantial or persistent breach of any warranties or undertakings given by it under this Agreement;

8.2.4 a final decision against which no further appeal is possible of a competent court or of the Data Protection Commission or other supervisory authority where appropriate rules that there has been a breach of this Agreement by the Data Controller or the Data Processor; or

8.2.5 a petition is presented for the administration or winding up of the Data Controller, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Processor is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs, then the Data Controller, without prejudice to any other rights which it may have against the Data Processor, shall be entitled to terminate this Agreement, in which case the Data Protection Commission or other supervisory authority where appropriate shall be informed where required.

8.3 The parties agree that the termination of this Agreement at any time, in any circumstances and for whatever reason (except for termination under Clause 8.2) does not exempt them from the obligations and/or conditions under this Agreement as regards the processing of the Personal Data transferred.

## **9. RETURN OR DESTRUCTION OF PERSONAL DATA**

9.1 The Data Processor shall, upon termination or expiry of this Agreement, or at any time, on the written request of the Data Controller:

- (i) not use, copy, disclose or otherwise Process any Personal Data and promptly return the Personal Data to the Data Controller; and
- (ii) if requested by the Data Controller, securely destroy all copies of the Personal Data received and/or processed by it under this Agreement unless the Law requires storage of the Personal Data.

The Data Processor shall, upon request, provide written confirmation to the Data Controller that the Personal Data has been returned or securely destroyed in accordance with this Clause.

## **10. COSTS AND EXPENSES**

10.1 The Parties shall pay its own costs, charges and expenses incurred in relation to the preparation, execution and carrying into effect of this Agreement.

## **11. WAIVER**

11.1 A failure by either Party to exercise and any delay, forbearance or indulgence by either Party in exercising any right, power or remedy under this Agreement shall not operate as a waiver of that right, power or remedy or preclude its exercise, at any subsequent time or on any subsequent occasion. The single or partial exercise of any right, power or remedy shall not preclude any other or further exercise of that right, power or remedy. No custom or practice of the Parties at variance with the terms of this Agreement shall constitute a waiver of the rights of either Party under this Agreement.

## **12. NOTICES**

12.1 Any notice required to be given under this Agreement shall be in writing and shall be served if hand delivered or sent by prepaid, recorded, or special delivery post or prepaid international recorded airmail, to the address and for the attention of the relevant Party set out in Clause 12.2 or at such other address as either Party may designate from time to time in accordance with this Clause.

12.2 The addresses of the Parties for the purposes of written notices are:

- (i) Data Controller:  
**The Land Development Agency**  
**George's Court,**  
**54-62 Townsend St,**  
**Dublin 2,**  
**D02 R156**

- (ii) Data Processor:  
[Organisation Name]  
[Organisation Registered Address]

or such other address as may be notified in writing from time to time by the relevant Party to the other. Any such change to the place of service shall take effect immediately after notice of the change is received or (if later) on the date (if any) specified in the notice as the date on which the change is to take place.

- 12.3 Any notice sent pursuant to this Clause 10 shall be deemed to have been served if hand delivered or sent by prepaid, recorded, or registered post or prepaid international recorded airmail, at the time of delivery.

## **13 LAW APPLICABLE TO THIS AGREEMENT**

This Agreement shall in all respects be governed by and interpreted in accordance with the laws of the Republic of Ireland. The parties hereto hereby submit to the exclusive jurisdiction of the Irish Courts for all the purposes of this Agreement.

## **14 VARIATION OF THIS AGREEMENT**

The parties may not modify this Agreement except to update any information in Schedule 1, in which case they will inform the Data Protection Commission or other supervisory authority where appropriate where required. This does not preclude the parties from adding additional commercial clauses where required and does not affect the Services Agreement between the Data Controller and the Data Processor. In cases where any conflict arises in the interpretation of these agreements, this Agreement shall take precedence.

**THIS AGREEMENT** has been signed on the date stated at the beginning of this Agreement.

**SIGNED** for and on behalf of The Land Development  
Agency, **Data Controller**

**SIGNED** for and on behalf of [Processor Name],  
**Data Processor**

**Signature**

\_\_\_\_\_

**Print Name**

\_\_\_\_\_

**Title**

\_\_\_\_\_

**Signature**

\_\_\_\_\_

**Print Name**

\_\_\_\_\_

**Title**

\_\_\_\_\_

## SCHEDULE 1

### DETAILS OF THE DATA PROCESSING ACTIVITIES

#### **PART A**

##### **Name of Parties and Roles**

| <b>Data Controller</b>             | <b>Data Processor</b>   |
|------------------------------------|-------------------------|
| <b>The Land Development Agency</b> | <b>[Processor Name]</b> |

#### **PART B**

##### **Data Subjects**

The Personal Data concerns the following categories of Data Subjects:

| <b>Categories of Data Subjects</b>                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[.....]</b><br><i>[Insert a description of the people whose data is being processed, e.g. service users, employees, commercial contacts, etc..]</i> |

#### **PART C**

##### **Categories of Personal Data**

The Personal Data concern the following categories of data:

| <b>Categories of Data</b>                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[.....]</b><br><i>[Insert a description of the sorts of data that may be transferred, e.g. name, contact details, date of birth, financial information, etc.]</i> |

#### **PART D**

##### **Special Categories of Personal Data**

The Personal Data concern the following categories of data:

## Special Categories of Data

[.....]

- *[racial or ethnic origin*
- *Political opinions*
- *Religious or philosophical beliefs*
- *Trade union membership*
- *Genetic data*
- *Biometric data*
- *Health information*
- *Data relating to sex life or sexual orientation*
- *Information relating to criminal charges or convictions*
- *N/A]*

## PART E

### Nature of the Processing:

The nature of the processing of Relevant Personal Data by the Processor **is the performance of the Services pursuant to the Services Agreement**, namely:

[.....]

*[Insert a clear description of the processing activities carried out in order to deliver the Services under the Services Agreement]*

## PART F

### Purpose of Processing

The purpose of the processing **is the performance of the Services by the Processor pursuant to the Services Agreement**, namely:

[.....] *[Insert the specific business purpose for which LDA is engaging the Processor (e.g. hosting, payroll administration, survey management, CRM support, etc.)]*

## PART G

### Sub-Processors

| Name    | Purpose | Location |
|---------|---------|----------|
| [.....] | [.....] | [.....]  |
| [.....] | [.....] | [.....]  |
|         |         |          |
|         |         |          |
|         |         |          |

## PART H

### Transfer of Personal Data to Third Countries

| Third Countries                                                                             | Strike through if not applicable                                                                                                               |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Country(ies) outside of the European Economic Area (EEA) where Personal Data is transferred | <div data-bbox="788 387 842 421" style="background-color: yellow; border: 1px solid black; display: inline-block; padding: 2px;">[.....]</div> |

## **SCHEDULE 2**

### **DATA PROCESSOR TECHNICAL, ORGANISATIONAL AND SECURITY MEASURES**

In accordance with Clause 4.4 of the Agreement, the Processor will adopt and maintain appropriate (including organisational and technical) security measures in dealing with Relevant Data in order to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In determining the technical and organisational security measures required, the Processor will take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Processor will implement the following specific security measures, as applicable:

- The Processor will establish, maintain, and comply with a written information security program that shall:
  - (i) meet the standards of good industry practice to safeguard Relevant Data;
  - (ii) identify appropriately defined organisational roles related to security and incident response;
  - (iii) ensure compliance with applicable data security and privacy laws;
  - (iv) protect against the destruction, loss, disclosure, alteration or other unauthorised processing of Relevant Data, in the possession of the Processor or to which the Processor may have access;
  - (v) include all reasonable precautions with respect to the employment of and access given to the Processor, including background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Relevant Data and in connection with the Processor's written information security program;
  - (vi) include an appropriate network security program (that includes, without limitation, encryption of all sensitive or private data and network and application partitioning), access identification and authentication, maintenance and media disposal, audit and accountability, physical and environmental protection, systems and communication security; and incident response and planning; and
  - (vii) meet or exceed the requirements of Applicable Data Protection Law.
- The Processor will establish, maintain, and comply with policies, procedures, and practices reasonably designed to protect its facilities, systems, and assets against external and internal threats, including, but not limited to, Internet or electronic-based threats, and to ensure the integrity and reliability of such facilities, systems, service, which shall include, to the extent appropriate:

- (i) critical asset identification;
- (ii) configuration and change management for software systems;
- (iii) physical and environmental protection; and
- (iv) contingency planning/redundancy.

- [Insert other appropriate security measures and obligations, such as:

## The below is provided as an example only

### 1. Organisational Measures

- **Data Protection Officer (DPO):** A qualified DPO is appointed and reachable at dpo@example.com.
- **Policies:** A suite of internal policies governs data handling, including a Data Protection Policy, Access Control Policy, and Incident Response Policy.
- **Training & Awareness:** All personnel undergo annual GDPR and cybersecurity training, with additional onboarding modules for new hires.
- **Third-Party Management:** Vendors are risk-assessed and bound by data processing agreements aligned with Article 28(3) GDPR.
- **Data Minimisation:** Data is collected and processed only as necessary for the stated purposes, with regular reviews.

### 2. Access Controls

- **Authentication:** MFA is enforced for all user accounts accessing personal data.
- **Role-Based Access Control (RBAC):** Access rights are granted on a need-to-know basis and regularly reviewed.
- **Logging & Monitoring:** Access to personal data is logged and monitored for anomalies.

### 3. Encryption and Data Security

- **Data in Transit:** TLS 1.2 or higher is used for all external communications.
- **Data at Rest:** Personal data stored in databases and backups is encrypted using AES-256.
- **Mobile Devices:** Laptops and smartphones are encrypted and remotely wipeable.

### 4. Availability and Resilience

- **Backup:** Daily encrypted backups are retained for 30 days. Backups are tested quarterly.
- **Business Continuity & Disaster Recovery (BC/DR):** A documented and tested BC/DR plan exists, including RTO < 8h and RPO < 4h for critical systems.

### 5. Incident Management

- **Breach Response:** A documented breach response plan is in place. Breaches are reported to the DPO within 12 hours and to authorities where required under Article 33 GDPR.
- **Security Incident Log:** All incidents are recorded, investigated, and remediated in a central logbook with root cause analysis.

## **6. Data Subject Rights**

- Procedures are in place to handle requests under Articles 15–22 GDPR (access, rectification, erasure, restriction, portability, objection) within the required timeframes.

## **7. Sub-Processor Oversight**

- Sub-processors are vetted for TOMs equivalence. An up-to-date list of sub-processors is maintained and shared with the controller.