Data Processing Agreement (DPA)

This **Data Processing Agreement** (the “**Agreement**”) is entered into by and between:

THE ULTIMA INVESTMENTS CYPRUS LIMITED, previously BrokerCreditService (Cyprus) Limited, a company incorporated and registered in the Republic of Cyprus with company number HE 154856, whose registered office is at Spyrou Kyprianou &1 Oktovriou, 1, VASHIOTIS KALANDE OFFICES, 1st floor, Mesa Geitonia, 4004, Limassol, Cyprus (the “**Ultima Cyprus”**);

and

The Company as identified in the NDA, and/or the General Terms for Dealing in Securities, and/or the General Terms, and/or any onboarding documentation (including but not limited to KYC forms). (the “**Counterparty**”, together with Ultima Cyprus – the **“Parties”**)

WHEREAS, the parties are in the process of establishing a commercial relationship, which may include onboarding, conducting due diligence (including KYC), negotiating, entering into and performing one or more potential agreements between them (the “**Commercial Relationship**”). In connection with this Commercial Relationship, both parties may exchange personal data as required under applicable data protection laws and regulations.

WHEREAS, the parties acknowledge that in some circumstances each acts as an independent controller, and in others one may act as a processor on behalf of the other.

WHEREAS, the parties wish to ensure that the processing is conducted in compliance with applicable Data Protection Laws, including the General Data Protection Regulation (GDPR) (EU) 2016/679 and other relevant legislation.

NOW, THEREFORE, in consideration of the mutual promises and covenants herein contained, the parties agree as follows:

1. Definitions

“Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

“EEA” means the European Economic Area.

“GDPR” means EU General Data Protection Regulation 2016/679.

“Data Transfer” means:

- a transfer of Personal Data from the Controller to a Processor; or
- an onward transfer of Personal Data from a Processor to a Sub-processor, or between two establishments of a Processor.

“Sub-processor” means any third party engaged by the Processor who agrees to receive from the Processor any Personal Data for processing on behalf of the Controller in accordance with this Agreement.

The terms, **“Commission”**, **“Controller”**, **“Data Subject”**, **“Member State”**, **“Personal Data”**, **“Personal Data Breach”**, **“Processing”** and **“Supervisory Authority”** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Roles and Scope

2.1 The Parties acknowledge that they may exchange Personal Data either:

a) as independent controllers, each determining the purposes and means of processing; or

b) as controller and processor, where one party processes data solely on documented instructions of the other.

2.2 The role of each Party with respect to each data exchange will be identified in the relevant annex to this Agreement or by context of the processing activity.

3. Controller-to-Controller Provisions

3.1 Where the Parties act as independent controllers:

(a) Each Party shall comply with its own obligations under the Data Protection Laws;

(b) Each Party shall provide Data Subjects with the required information under Articles 13 and 14 of the GDPR;

(c) Each Party shall establish a lawful basis for the processing and sharing of data;

(d) The Parties agree to assist each other, where feasible, in handling requests from Data Subjects and regulatory authorities.

4. Controller-to-Processor Provisions

Where one Party acts as Processor on behalf of the other (the Controller), the provisions of Schedule A shall apply.

5. Standard Contractual Clauses

5.1 Where the processing of Personal Data involves a transfer to a country outside the European Economic Area that does not benefit from an adequacy decision under applicable Data Protection Laws, the Parties agree that the EU Standard

Contractual Clauses adopted by the European Commission on 4 June 2021, including their Annexes I–III, shall apply. The SCCs are attached to this Agreement as Schedule B and form an integral part hereof. For the purposes of the SCCs, the roles of the Parties (Controller–Controller or Controller–Processor) shall be as set out in the relevant Module and in the applicable Schedule to this Agreement.

5.2 For the purposes of the SCCs, Annex I identifies the Data Exporter and the Data Importer. The Data Importer is the counterparty accepting this Agreement, as identified in the NDA, and/or the General Terms for Dealing in Securities, and/or the General Terms, and/or onboarding documentation or other written agreement between the Parties.

6. Confidentiality

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

7. Termination

7.1 This Agreement shall terminate automatically upon the termination of the Commercial Relationship.

7.2 Upon termination, the Processor shall, at the choice of the Controller, delete or return all the Personal Data to the Controller and delete existing copies unless required by law to retain such data.

8. Governing Law and Jurisdiction

8.1 This Agreement shall be governed by and construed in accordance with the laws of Cyprus.

8.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Cyprus.

9. Accession by Reference

By accepting the NDA, and/or the General Terms for Dealing in Securities, and/or the General Terms, and/or other onboarding documentation referring to this Agreement, the Counterparty confirms its accession to and acceptance of this Agreement, including the

Standard Contractual Clauses in Schedule B, to the extent applicable to the relationship and roles of the Parties under the relevant data processing context..

Schedule A

Terms of Processing

This Schedule A forms an integral part of the Agreement and applies where and to the extent the Counterparty processes Personal Data on behalf of Ultima Cyprus as a Processor under Article 28 GDPR.

1. Subject Matter of Processing

The Processor shall process Personal Data hereunder exclusively within the scope of the Commercial Relationship under which the Processor provides certain services to the Controller, which may require the Processor to process personal data on behalf of the Controller, including the execution of necessary KYC and due diligence procedures as required under applicable laws and regulations.

2. Duration of Processing

The processing of Personal Data shall continue for the duration of the Commercial Relationship, or until such data is returned or deleted as instructed by the Controller.

3. Nature of Processing

3.1 The nature of the processing includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. Types of Personal Data

The types of Personal Data processed may include but are not limited to:

- Name (name and surname)
- Personal identity number
- Identity document photo
- Date of birth
- Nationality
- Gender
- User name
- E-mail address
- Telephone number
- Residence or Shipment address

- Salary and other sources of income
- Employment terms (incl salary and benefits)

5. Categories of Data Subjects

The categories of Data Subjects may include but are not limited to:

- Candidate
- Employee;
- Director;
- Services provider being natural person;
- Employee, director, representative of services provider being entity;
- Client/counterparty being natural person;
- Employee, director, secretary, representative, shareholder, beneficiary of client/counterparty being entity;
- Employee, director, representative, shareholder, beneficiary of client`s/counterparty`s director being entity.

6. Obligations of the Processor

6.1 The Processor agrees to:

6.1.1 Process Personal Data only on documented instructions from the Controller.

6.1.2 Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.

6.1.3 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

6.1.4 Assist the Controller in ensuring compliance with its obligations under the GDPR.

6.1.5 At the choice of the Controller, delete or return all Personal Data after the end of the provision of services, and delete existing copies unless required by law.

6.1.6 Provide the Controller with confirmation of the completed data deletion.

6.1.7 Make available to the Controller all information necessary to demonstrate compliance with this Agreement.

6.2 With the Controller’s consent, the Processor may use false information for the purpose of anonymizing client personal data. The false data must be securely integrated into the system to eliminate any possibility of re-identification. The Processor is obliged to ensure that the use of false information does not lead to any legal implications for the Controller.

7. Sub-processing

The Processor shall not engage another processor without prior specific or general written authorization of the Controller. In the case of general written authorization, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors.

8. Data Subject Rights

8.1 Considering the nature of the Processing, Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

8.2 Processor shall:

8.2.1 promptly notify the Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

8.2.2 ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the Processor responds to the request.

9. Data Breach

9.1 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data breach, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2 Processor shall co-operate with the Controller and take reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. Audit

10.1Subject to this section 10, Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Personal Data by the Processors.

10.2Information and audit rights of the Controller only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. International Transfers

The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

Schedule B

Standard Contractual Clauses for Personal Data Transfers between EU Controller and Third-Country Controller and/or Processor (Controller-to-Controller Transfer and Controller-to-Processor Transfers)

The Parties agree that these Clauses incorporate:

- Module One (Controller to Controller), and
- Module Two (Controller to Processor).

The applicable Module shall be determined for each data transfer as specified in Annex I.

Clauses 1 to 18 of the Standard Contractual Clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 of 4 June 2021 are incorporated herein by reference and form an integral part of this agreement.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: THE ULTIMA INVESTMENTS CYPRUS LIMITED, previously BrokerCreditService (Cyprus) Limited

Address: Spyrou Kyprianou & 1 Oktovriou, 1 VASHIOTIS KALANDE OFFICES, 1st floor, Mesa Geitonia, 4004 Limassol, Cyprus

Contact person's name, position and contact details:

Igor Zatseda, Executive Director responsible for regulatory compliance and AML matters, tel: +357 25 822734; E-mail address: compliance.cy@theultimagm.com; Data Protection Officer: REG4TECH LTD, Contact person: Demos Demou, Engagement Partner, E-mail address: dpo.cy@theultimagm.com

Activities relevant to the data transferred under these Clauses:

The Data exporter provides the investment services and activities pursuant to the license No 048/04 issued on 08 October 2004 by the Cyprus Securities and Exchange Commission.

The processing is carried out for the purposes of onboarding, conducting due diligence (including KYC), contract negotiation, execution and performance of one or more potential commercial agreements between the Parties.

Data importer(s):

The Counterparty, as identified in the NDA, and/or the General Terms for Dealing in Securities, and/or the General Terms, and/or onboarding documentation

B. DESCRIPTION OF TRANSFER

Transfer 1: Controller to Controller (Module One applied Controller to Controller)

Transfer 2: Controller to Processor (Module Two applied Controller to Processor)

Categories of data subjects whose personal data is transferred (applies to both transfers)

- Candidate
- Employee;
- Director;
- Services provider being natural person;
- Employee, director, representative of services provider being entity;

- Client/counterparty being natural person;
- Employee, director, secretary, representative, shareholder, beneficiary of client/counterparty being entity;
- Employee, director, representative, shareholder, beneficiary of client`s/counterparty`s director being entity.

Categories of personal data transferred (applies to both transfers)

- Name (name and surname)
- Personal identity number
- Date of birth
- Nationality
- Gender
- User name
- E-mail address
- Telephone number
- Customer number
- Tax number
- Residence address

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

1. Participation in a body, association and trade union;
2. Health;
3. Data relevant to criminal prosecutions or convictions.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

On continuous basis.

Nature of the processing

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing

Provision of services under the Commercial Relationship specified above.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The retention period will be determined taking into consideration the legislative and regulatory requirements and legal risks of the company where data may be necessary for the establishment, exercise or defence of legal claims.

C. COMPETENT SUPERVISORY AUTHORITY

Cyprus Commissioner for Personal Data Protection

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Appendix forms part of the agreement and describes the technical and organisational security measures implemented by the Data importer in accordance with clauses 4(d) and 5(c):

1. Vulnerability and Incident Management

- The Data Importer will conduct bi-annual Vulnerability Assessment and Penetration Testing (VAPT) to evaluate application security and address high and medium vulnerabilities. The Data Importer also periodically reviews the adequacy of these security measures to stay current with evolving risks.
- The Data Importer will inform the Data Exporter of any suspicious activity indicating potential data leakage and will monitor privileged user activities related to end-customer data access. In case of a security incident, the Data Importer will report to the Data Exporter within three days after recovery from the incident.
- Security configuration changes related to the Data Exporter's application will be reported upon request.
- The Data Importer's staff will monitor compliance with information security policies and ensure that employees are trained on maintaining information security.

2. Confidentiality and Data Access Control

- Access to Data Exporter information will be restricted based on the principle of "need to know" and "need to perform," using strict user access controls and password protection.
- The confidentiality of Data Exporter information is preserved at the application, database, and network levels through standardized security tools. The Data Importer has a user authorization system in place to regulate access to information resources, databases, and files containing personal data.
- Employees are bound by non-disclosure clauses in their employment contracts, and policies are regularly reviewed and customized to the Data Exporter's needs.

3. Physical and Logical Data Integrity

- The Data Importer ensures both physical and logical integrity of Data Exporter information. Hardware and network equipment are physically secured, and data integrity is maintained to prevent unauthorized changes during processing, storage, or transmission.
- Physical security measures include secure doors, locks, CCTV, supervised visitor access, secure disposal of paper waste, and protection for portable and removable

media. Equipment processing personal data is housed in secure areas, with regular checks for unauthorized access.

4. **Computer and Network Security**

   - Weekly backups of personal data are stored on secure media to enable data recovery in case of corruption or loss.
   - Firewalls and secure links protect the data, with an SSL-secured URL for the Data Importer's applications to enhance connection security. VPN connections are used between the Data Importer and Data Exporter offices to ensure the confidentiality of data transmission.
   - The Data Importer will implement industry best practices for web-facing applications, including protection against DDoS attacks, bot attacks, and common web vulnerabilities like cross-site scripting (XSS) and SQL injection.

5. **Data Segregation and Legal Compliance**

   - Data Exporter information is segregated at the application level to reduce risks of data leakage between institutions.
   - The Data Importer commits to safeguarding Data Exporter information even in legal scenarios (such as acquisitions, mergers, bankruptcies, or regulatory actions) that may impact the Data Exporter's operations. In such cases, the Data Importer will coordinate with regulatory authorities to ensure the Data Exporter retains access to its data.

6. **Compliance with Standards and Security Policy Implementation**

   - The Data Importer adheres to an IT Security Policy covering areas like passwords, information encryption, data sensitivity, and risk assessment, ensuring alignment with ISO/IEC 27001:2013 standards at a minimum.
   - The Data Importer mandates that any engaged sub-processors meet security standards no less stringent than those outlined in these measures.
   - The Data Importer will support the Data Exporter by providing information required by IT auditors or regulatory authorities.

7. **Continuous Improvement and Security Patches**

   - Security policies are structured, measurable, and undergo continuous assessment and improvement based on the Data Exporter's feedback.
   - The Data Importer will promptly implement security patches to maintain up-to-date security for Data Exporter systems.

Where the Data importer engages the sub-processor it shall ensure that the sub-processor applies the measures not less strict than those provided in these Clauses.

ANNEX III

LIST OF SUB-PROCESSORS

Annex III applies only where the Data Importer acts as a Processor