Data Processing Agreement

This Data Processing Agreement (the **"Agreement"**) is between the Customer and the Supplier (the **"Parties"**) and shall take effect and become binding between them:

- As per the Terms (the **"Principle Agreement"**) entered into between the Parties for the Services;
- to the extent that the Supplier processes Customer Personal Data for which they are deemed Data Controllers;
- and where this Agreement is required under the applicable Data Protection legislation.

For the purpose of the Data Protection Law, the Parties acknowledge that the Customer is the Controller and that the Supplier is the Processor in respect of any Personal Data.

This Agreement sets out the additional terms and conditions under which the Processor will process Personal Data on behalf of the Controller when providing Services under the Principle Agreement.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1. Definitions

Business Purposes means the services described in the Principle Agreement or any other purpose specifically identified in the Data Protection Schedule.

Controller means the entity that determines the purposes and means of the processing of Personal Data.

Data Protection Laws means any data protection and privacy laws applicable to the processing of Personal Data under this Agreement including EU Data Protection Law and, to the extent applicable, the data protection or privacy laws of any other country.

Data Protection Schedule means the document signed by the Parties setting out the detail and specifics of the Processing as required by this Agreement.

Data Subject means an individual who is the subject of Personal Data.

EU Data Protection Law means both (i) Directive 94/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive"); and (ii) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").

Personal Data means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Principle Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Process means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as 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.

Processor means the entity that processes Personal Data on behalf of a Controller, in this case the Supplier.

Standard Contractual Clauses (SCC) means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, details of which are included in Annexure A.

Sub-processor means any person (including any third party and any Processor Affiliate, but excluding an employee of the Processor) appointed by or on behalf of the Processor to Process Personal Data on behalf of the Controller in connection with the Principal Agreement; and

Services means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Controller pursuant to the Principal Agreement.

Supervisory Authority means an independent public authority which is (i) established by a European Union member state pursuant to Article 51 of the GDPR; or (ii) the public authority governing data protection, which has supervisory authority and jurisdiction over Controller.

1.2. This Agreement is subject to the terms of the Principle Agreement and is incorporated into the Principle Agreement.

1.3. The Annexes to this Agreement and the Data Protection Schedule form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4. Clause, annexure and paragraph headings shall not affect the interpretation of this Agreement.

1.5. A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.

1.6. Where the words include(s), including or in particular are used in this Agreement, they are deemed to have the words without limitation following them. Where the context permits, the words other and otherwise are illustrative and shall not limit the sense of the words preceding them.

1.7. In the case of conflict or ambiguity between:

a. any provision contained in the body of this Agreement and any provision contained in the Annexes or the Data Protection Schedule, the provision in the body of this Agreement will prevail;

b. the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes and Data Protection Schedule, the provision contained in the Annexes and Data Protection Schedule will prevail;

c. any of the provisions of this Agreement and the provisions of the Principle Agreement, the provisions of this Agreement will prevail; and

d. any of the provisions of this Agreement and any applicable SCC, the provisions of the applicable SCC will prevail.

2. OBLIGATIONS, PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1. The Data Protection Schedule describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Processor may process the Personal Data to fulfil the Business Purposes of the Principle Agreement.

2.2. The Controller's written authorisation is required to process the Personal Data or for transferring the Personal Data to any country or international organisation as reasonably necessary for the provision of the Services and must be consistent with the Principal Agreement and Business Purpose.

2.3. Obligations of the Controller:

a. The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Law, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Processor.

b. The Controller shall refrain from providing instructions which are not in accordance with applicable laws including Applicable Data Protection law, and, in the event that such instructions are given, the Processor is entitled to resist carrying out such instructions.

2.4. Obligations of the Processor:

a. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Law. The Processor must promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Law.

b. The Processor will keep detailed, accurate and up-to-date records regarding any processing of Personal Data it carries out for the Controller. The Processor will ensure that the Records are sufficient to enable the Controller to verify the Processor's compliance with its obligations under this Agreement and the Processor will provide the Controller with copies of the Records upon reasonable request.

c. Processor must promptly comply with any Controller's request or instruction requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

d. The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

e. The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Law, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Law.

f. The Processor must promptly notify the Controller of any changes to Data Protection Law that may adversely affect the Processor's performance of the Principle Agreement.

3. PROCESSOR EMPLOYEES AND AFFILIATED PERSONNEL

3.1. The Processor will ensure that all employees or persons authorised to process the Persona Data:

a. Are advised of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of this Personal Data; and

b. Are aware of both the Processor's duties and their personal duties and obligations under the Data Protection Law and this Agreement.

3.2. The Processor will take reasonable steps to ensure the reliability of any employee or authorised person who may have access to the Personal Data.

3.3. The Processor will ensure that access to the personal data is granted only to the extent that this is necessary for the performance of the data processing operations as instructed by the Controller.

3.4. The Processor will ensure that any authorised person who has access to the Personal Data does not process it except on instruction.

4. SUB-PROCESSORS

4.1. The Processor shall not appoint a third party (Sub-processors) to process Personal Data unless it has received written consent from the Controller.

4.2. The Processor must enter into a written contract with the Sub-processor that contains terms substantially the same as those set out in this Agreement, providing sufficient guarantees that appropriate technical and organisational measures will be implemented when Processing the Personal Data. The Processor should exercise control over all Personal Data it entrusts to the Sub-processor.

4.3. Those Sub-processors approved as at the commencement of this Agreement are set out in the Data Protection Schedule.

4.4. Where the Processor has engaged a Sub-processor, the Processor shall be fully liable for the fulfilment of all obligations by the Sub-processor.

5. SECURITY

5.1. Both the Processor and the Controller shall at all times maintain, evaluate and, where necessary, adapt and update appropriate technical and organisational measures to protect against any form of unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures are found at **https://valiantys.com/legal/trust** .

5.2. Such measures guarantee, taking into account the nature, scope, context and purposes of processing, the state of the art and the cost of implementation, an appropriate level of security in view of the risks of varying likelihood and severity entailed by the processing of the data to be protected, and are in accordance with the provisions of the guidelines and Article 32 of the GDPR. They further include as appropriate:

a. the pseudonymisation and encryption of Personal Data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services the ability to restore the availability;

c. and access to Personal Data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of security measures.

5.3. At the Controller's request, the Processor shall make all information available that is necessary to prove that the provisions of this clause 5 have been complied with.

6. PERSONAL DATA BREACH

6.1. The Processor shall notify the Controller without undue delay upon the Processor becoming aware of a Personal Data Breach affecting the Personal Data. It must provide the Controller with sufficient information to allow the Controller to meet any obligations to report or inform the Data Subjects of the Personal Data Breach or the Supervisory Authority under the Data Protection Laws.

6.2. Such notification shall as a minimum:

a. describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
b. communicate the name and contact details of the Processor's data protection officer or other relevant contact from whom more information may be obtained;
c. describe the likely consequences of the Personal Data Breach; and
d. describe the measures taken or proposed to be taken to address the Personal Data Breach.
6.3. The Processor shall co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

6.4. The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controller's prior written consent, except when required to do so by law.

6.5. The Processor agrees that the Controller has the sole right to determine:

a. whether to provide notice of the Personal Data Breach to any Data Subjects, Supervisory Authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice; and

b. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. DATA IMPACT ASSESSMENT

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of the Controller by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available.

8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

8.1. The parties agree that this subsection shall apply only to Personal Data that is protected by Data Protection Legislation and such Personal Data is transferred outside the European Economic Area (EEA) to the Processor, either directly or via onward transfer.

8.2. The Processor will only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

a. the Processor is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Law that the territory provides adequate protection for the privacy rights of individuals. The Processor must identify in the Data Protection Schedule the territory that is subject to such an adequacy finding; or

b. the Processor participates in a valid cross-border transfer mechanism under the Data Protection Law, so that the Processor (and, where appropriate, the Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR. The Processor must identify in the Data Protection Schedule the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Processor must immediately inform the Controller of any change to that status; or

c. the transfer otherwise complies with the Data Protection Law for the reasons set out in Data Protection Schedule.

8.3. The terms of the Standard Contractual Clauses outlined in Annexure A will apply where the applicable transfer of Customer Personal Data is (a) not subject to the laws of a jurisdiction recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Legislation); or (b) not covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. In the event of any conflict or inconsistency between the provisions of this Addendum and the Standard Contractual Clauses outlined in Annexure A, the provisions of the Standard Contractual Clauses shall prevail. In the event that any provision of the Standard Contractual Clauses is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of the Standard Contractual Clauses and the terms of this Addendum shall remain operative and binding on the parties.

8.4. If the Controller consents to appointment by the Processor located within the EEA of a Sub-processor located outside the EEA in compliance with the provisions of clause 8, then the Controller authorises the Processor to enter into SCC contained in Annexure A with the Sub-processor on its behalf. The Processor will make the executed SCC available to the Controller on request.

9. DATA SUBJECT RIGHTS

9.1. Taking into account the nature of the Processing, the Processor shall, assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, to enable the Controller to respond to requests to exercise Data Subject rights under the Data Protection Law.

9.2. The Processor shall:

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

b. give the Controller its full co-operation and assistance in responding to any Data Subject request; and

c. not disclose the Personal Data to any Data Subject or to a third party other than at the Controller's request or instruction, as provided for in this Agreement or as required by law.

10. TERM AND TERMINATION

10.1. This Agreement will remain in full force and effect so long as:

a. the Principle Agreement remains in effect; or

b. the Processor carries out Personal Data processing operations or retains Personal Data on behalf of Controller (**"Term"**).
10.2. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Principle Agreement in order to protect Personal Data will remain in full force and effect.

10.3. Failure to comply with the terms of this Agreement is a material breach of the Principle Agreement.

11. DATA RETURN AND DESTRUCTION

11.1. Upon instruction by the Controller or termination or expiry of the Principle Agreement, the Processor will either:

a. give the Controller a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller; or

b. will delete and procure the deletion of all copies of the Personal Data and demonstrate to the satisfaction of the Controller that it has taken such measures.

11.2. At the request of Controller, the Processor shall return and not retain, the Personal Data in its possession or control.

11.3. If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

12. AUDIT

12.1. The Processor shall make available to the Controller or its third-party representative all information required to demonstrate compliance with this Agreement in relation to the process of Private Data. This may be accomplished through annual audits or inspections by the Controller on at least 14 days written notice to the Processor at any time during the term of this Agreement.

12.2. The Processor shall give every assistance to that end and provide in a timely manner such information relevant to the audit as is necessary to be able to prove compliance with the obligations contained in Article 28 of the GDPR.

12.3. The notice requirements in clause 12.1 will not apply if the Controller reasonably believes that a Personal Data Breach occurred or is occurring, or the Processor is in breach of any of its obligations under this Agreement or any Data Protection Law.

12.4. The Controller shall appoint an audit representative to undertake the audits. When undertaking an audit, the Controller shall make reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The Controller shall also abide by all security and safety measures in place on the Processor's premises. The Processor need not give access to its premises for the purposes of such an audit or inspection is performed outside of normal business hours, unless the audit or inspection needs to be conducted on an emergency basis and the Controller has given notice to the Processor.

12.5. The costs of an audit are payable by the Controller, unless the audit shows that the Processor has acted contrary to this agreement or has failed to take appropriate measures, taking into account the state of the art and the cost of implementation, in view of the risks entailed by the processing, the nature, the scope, the context and the purposes of the data to be protected.

12.6. If a Personal Data Breach occurs or is occurring, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Law, the Processor will:

a. promptly conduct its own audit to determine the cause;

b. produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

c. provide the Controller with a copy of the written audit report; and

d. remedy any deficiencies identified by the audit as soon as possible.

12.7. At the Controller's written request, the Processor will:

a. conduct an information security audit before it first begins processing any Personal Data and repeat that audit on an annual basis;

b. produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

c. provide the Controller with a copy of the written audit report; and

d. remedy any deficiencies identified by the audit within as soon as possible.

12.8. On the Controller's written request, the Processor will make all of the relevant audit reports available to the Controller for review. The Controller will treat such audit reports as the Processor's confidential information under this Agreement.

13. INDEMNIFICATION

Each Party indemnifies the other, at its own expense, against all costs, claims, damages or expenses incurred by a Party due to any failure by the other Party to comply with any of its obligations under this Agreement or the Data Protection Law.

14. DISPUTE RESOLUTION AND GOVERNING LAW

The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

15. NOTICES

Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to the addresses set out in Data Protection Schedule.

16. SEVERANCE

If any court or competent authority finds that any provision or part of this Agreement is invalid, illegal or unenforceable, that provision or part shall, to the extent required, be deemed to be deleted, and the remaining provisions of this Agreement shall continue in full force and effect.

17. VARIATION

No variation of this Agreement (or any document referred to in it) shall be effective unless it is in writing and signed by, or on behalf of, each of the Parties to this Agreement.

ANNEXURE A: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses for the transfer of personal data from the European Union to processors established in third countries (controller to processor transfers).

The EU Standard Contractual Clauses are available at the following link **http://data.europa.eu/eli/dec/2010/87/oj** The Parties hereby agree that by reference to this link the EU Standard Contractual Clauses shall be deemed incorporated into this Data Processing Agreement and made an integral part of it.

Appendix 1 and 2 to the Standard Contractual Clauses

Data exporter: Customer

Data importer: Valiantys

The Details of the Data subjects, Categories of data, Special categories of data (if appropriate), Processing operations and the technical and organisational security measures are set out in the Data Protection Schedule entered into between the Parties.