INTRODUCTION

It is a legal requirement under the GDPR to ensure a data processing agreement (DPA) is in place between a Data Controller and Data Processor. This DPA works in conjunction with Glantus Standard Contractual Clauses (SCCs) and adopts the modular approach when defining the relationship between Controllers and Processors.

CUSTOMERS

Glantus' customers have primary responsibility as **controllers** for the personal data they share with Glantus as the Data Processors.
Glantus' services involve only limited processing of personal data on behalf of our customers (e.g., contracted information included on invoices or to maintain the services provided)

If a DPA has not been supplied by the customer this agreement can form a mutual DPA.

SUPPLIERS

Glantus' suppliers have a responsibility as **processors** to comply with the GDPR and protection of personal data where Glantus is the Data Controller.
While data controllers generally assume a greater degree of responsibility for ensuring the protection of personal data, they share with data processors, both controllers and processors are subject to the requirement to implement a GDPR-compliant data processing agreement. It is therefore important that Glantus has a data processing agreement in place with our suppliers and with our customers.

PURPOSE

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Solutions and/or Services ("**Principal Agreement**") between ***Data Controller and Data Processor within the meaning of the General Data Protection Regulation (GDPR EU) and General Data Protection Regulation (GDPR UK), to provide solutions and/or services that require the processing of personal information. The following terms (the "Data Processing Agreement") are hereby incorporated in addition to the Terms and Conditions under which services are provided and form part of the contract for those solutions and/or services.***

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**"). Details of processing activities are to be completed in **Annex I** of this document.

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

_____
(the "Company", Data Controller) and

Glantus
_____
(the "**Data Processor**") (together as the "**Parties**") **WHEREAS**

Data Controller: Is the owner of the information.

Data Processor: Is the provider of the service or product.

CONTEXT

The Company acts as a Data Controller.

(A) The Data Controller wishes to subcontract certain Services and/or Solutions, which imply the processing of personal data, to the Data Processor.

(B) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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 (General Data Protection Regulation) or equivalent compatible regulation (e.g., CCPA) based on local jurisdiction in accordance with ISO:27701 standard.

(C) The Parties wish to lay down their rights and obligations.

SCOPE

The Agreement applies to solutions and/or services sought for which Glantus Group, operating under the name 'Glantus', is acting as a Data Processor and Customer is acting as a Data Controller within the meaning of the Regulation.
The Agreement also applies where 'Glantus' are controllers and services are being sought from data processors.
The agreement covers Glantus as data controller where The Controller Personal Data may be consolidated to improve efficiency across data systems (e.g CRM) or if systems become redundant. The data subject will be contacted in such event. Such transfer of The Controller Personal Data is solely for operational purpose and legitimate interest to provide services as contracted to support the company's commitment to information security and data privacy.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules and Terms and Conditions

1.1.2 "**The Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement.

1.1.3 "**Contracted Processor**" means a Sub processor.

1.1.4 **"Data" or "Information"** shall refer to personal data pertaining to one or more data subjects as defined by the GDPR and DPA 2018.

1.1.5 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other jurisdiction holding an EU adequacy decision.

1.1.6 "**EEA**" means the European Economic Area.

1.1.7 "**GDPR EU**" and "**EU Data Protection Laws**" means EU General Data Protection Regulation 2016/679.

1.1.8 "**GDPR UK**" and "**UK Data Protection Laws**" means UK General Data Protection Regulation effective 1st January 2021

1.1.9 "**Data Transfer**" means:

1.1.9.1 a transfer of The Controller Personal Data from the Company to a Contracted Processor; or

1.1.9.2 an onward transfer of The Controller Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

1.1.10 **"Services"** means the solution or services the Company provides.

1.1.11 **"Controller"** shall refer to the Company acting as Data Controller as defined by the Regulation.

1.1.12 **"Processor"** shall refer to the supplier acting as Data Processor as defined by the Regulation.

1.1.13 **"Sub processor"** means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.1.14 "**Standard Contractual Clause**" or ("**SCCs**") means the standard contractual clauses approved by the European Commission for the transfer of personal data to processors established in countries which do not ensure an adequate level of data protection.

1.2 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. Processing of The Controller Personal Data

2.1 Processor shall:

2.1.1 Comply with all applicable Data Protection Laws in the Processing of The Controller Personal Data; and

2.1.2 Not Process the Controller Personal Data other than on the relevant Company's documented instructions.

2.2 The Controller instructs Processor to process The Controller Personal Data.

2.3 The Controller Personal Data may be consolidated to improve efficiency of company systems. In such case this is only to improve operational procedures.

3. Processor Personnel

3.1 Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant The Controller Personal Data, as strictly necessary for the purposesof the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings (NDA) or professional or statutory obligations of confidentiality relating to information security and privacy in line with Article 28 (GDPR).

4. Security

4.1 Taking into account 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, Processor shall in relation to the Controller Personal Data implement appropriate technical and organisational measures to ensure a level of information security and privacy appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Details of these technical and organisational measures are to be provided in **Annex II** of this agreement.

4.2 In assessing the appropriate level of security, Processor shall take account of the risks that are presented by Processing, in particular, from a Personal Data Breach.

5. Sub-processing/Sub-processors

5.1 Please provide details of sub-processors who will have access to The Controller personal data in **Annex III** of this agreement. Sub-processors included in Annex III of this document are deemed accepted by the controller in the terms of this agreement.

5.2 The Processor is responsible for ensuring that any sub-processors it uses to process data, must ensure processing is conducted in a secure and responsible manor in line with technical and organisational measures outlined by in **Annex II** by The Processor.

5.3 Processor shall not appoint (or disclose any Controller Personal Data to) any new Sub processor unless required or authorised by The Controller (Data Controller).

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist The Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of The Controller obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 As between the parties, the Controller is solely responsible for obtaining, and has obtained or will obtain, all necessary consents, licenses and approvals for the processing, or otherwise has a valid legal basis under Data Protection Laws for the Processing of Personal Data (the "Customer Legal Basis Assurance"). Without limiting the Customer Legal Basis Assurance, each Controller and Processor warrant in relation to Personal Data that it will comply with (and will ensure that any of its personnel comply with), the Data Protection Laws applicable to it.

6.3 Processor shall:

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

6.3.2 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 Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify The Controller without undue delay upon Processor becoming aware of a Personal Data Breach affecting The Controller Personal Data, providing Company 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 in line with Article 33 and 34 of the GDPR. An internal security incident report will be required in this instance. This can be made available to relevant parties if and when required.

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

7.3 The Processor will promptly provide the Controller with information regarding the breach including:

I. The nature of the personal data breach
II. The categories and approximate number of data subjects concerned
III. The categories and approximate number of personal data records concerned
IV. The likely consequences of the personal data breach
V. A summary of the unauthorised recipients of the personal data and,
VI. The measures taken or proposed to be taken by the Processor to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

8. Data Privacy Impact Assessment and Prior Consultation

8.1 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 Company reasonably considers to be required 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 The Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of The Controller Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of The Controller Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those The Controller Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within the time period as agreed.

10. Audit rights

10.1 Subject 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 Controller Personal Data by the Contracted Processors.

10.2 Information 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. Data Transfer

11.1 The Processor may not transfer or authorise 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 is adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 **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.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address

set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the applicable laws as per jurisdiction of the Data Subject or Company (Customer) location e.g. GDPR (The European Union), UK GDPR (England, Wales etc).

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the relevant courts of appeal.

13.3 The Data Subject may in some circumstances, hold the right to select the governing law and choice of jurisdiction of any EU member state. This depends on the origin or data and the location of processing.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Please specify 'Controller' or 'Processor' in the blanks below:

Data _Controller_ Company:

Signature:_____

Name:_____

Title:_____

Date Signed: _____

Data _Processor_ Company: Glantus

Signature: John Robinson

Name: John Robinson

Title: Group Compliance Manager and DPO

Date Signed: _____

ANNEX I: DESCRIPTION OF PERSONAL DATA PROCESSING

Annex I describes Vendor's processing of Company Personal data, in accordance with Section 2 of this DPA and Data Protection Laws.

Subject matter, duration, nature, and purposes of personal data processing:

Vendor shall process Company Personal Data to provide the Services set forth in the Service Agreement. Vendor's Processing of Company Personal Data shall terminate upon the destruction or return of Company Personal Data. Data is only held for the duration of an active contract.

Categories of personal data:

Standalone Name; Work email address; Employer name

Work physical address; Work phone number when combined with the above data can be categorised as personal data.

Categories of data subjects:

Employees of Customer for Customer Relationship Management (CRM)

Vendors of Customer to fulfil contract obligations.

ANNEX II: DESCRIPTION OF VENDOR'S SECURITY MEASURES

Annex II describes the technical and organizational security measures that Vendor has implemented in accordance with Section 4 of this DPA and Data Protection Laws.

Vendor information below:

Glantus implement appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Company Personal Data and ensure a level of security appropriate to the risk associated with the Processing activity, including, at a minimum, the measures referred to in Article 32(1) of the GDPR;

Implement and maintain appropriate security measures in accordance with good industry practice in the country or countries in which Vendor is Processing Company Personal Data and in accordance with the requirements of all Data Protection Laws;

Use encryption methods to safeguard Company Personal Data while in transit; and

Regularly monitor compliance with such security safeguards and ensure that there is no material decrease in the level of security afforded to Company Personal Data during the duration of the Processing.

Please see a link for the Datacentres we use in Marlborough, MA (US customer data only) which are ISO27001 and PCI DSS rated. The equipment located in the datacentre is wholly owned and managed by Glantus. Access to the equipment is managed by an approved lists of employees. Also we make extensive use of the Microsoft Azure platform.

All Communication to our infrastructure is fully encrypted using SSL/TLS to dedicated Frontend servers or services.

Servers holding any data, sit within a segregated Network, away from the frontend network housing the frontend servers. Communication between these networks is strictly controlled and there is no Direct access from the internet to the Network on which the Data resides.

All of the above sits behind a pair of Highly available, Load Balanced Firewalls, that protect the Exterior perimeter of the network and controls access between the individual network segments. At no point is unencrypted data transmitted outside the System.

Glantus user access to any systems/networks is further secured by the use of Multifactor Authentication where possible.

Data is backed up nightly to an encrypted backup, and a test restore is performed every month on a random server and file selection.

All of the above is monitored constantly for operational performance and anomalous behaviour is highlighted and alerted upon.

In addition, a Risk Committee meets at regular intervals to assess risk in various areas of the company including Information Security.

ANNEX III: List of Sub-Processors

Please provide a list of sub-processors who will have access to controllers personal data as described in section 5 of this agreement.

Azure – Microsoft – Cloud Storage – Retention for duration of project.

Office365 – Microsoft – Email, Collaboration, communication etc. – Retention is governed by subject access request under GDPR.