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 the customers (e.g., contracted information included on invoices or to maintain the services provided)

PURPOSE

This Data Processing Agreement ("**Agreement**") forms part of and is hereby incorporated in the Contract for Solutions and/or Services or Master Services Agreement ("**Principal Agreement**") between ***Data Controller and Data Processor within the meaning of the General Data Protection Regulation (GDPR EU) and UK General Data Protection Regulation (GDPR UK), to provide solutions and/or services that require the processing of personal information.***

Details of processing activities are completed in **Annex I** of this document.

This **Agreement** forms part of **Principal Agreement** between

Data Controller: Is responsible for the personal data.

Data Processor: Is the provider of the service or product, processing personal data on behalf of the Data Controller.

_____ (the "Company", Data Controller) and

Glantus _____

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

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, General Data Protection Regulation (GDPR) or equivalent compatible regulation (e.g., CCPA) based on local jurisdiction

(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.

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 Annexes, Schedules and Terms and Conditions.

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

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

1.1.4 "**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.

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

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

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

1.1.8 "**Data Transfer**" means a transfer of The Controller Personal Data for processing under this Agreement in a country which does not ensure an adequate protection of personal data in accordance with Data Protection Laws.

1.1.9 **"Services"** means the solution or services the Company provides under the Principal Agreement.

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

1.1.11 **"Processor"** shall refer to Glantus (including any of Glantus Group

companies) acting as Data Processor as defined by the Regulation.

1.1.12 **"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.

1.1.13 "**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 for the purposes described in Annex I to this Agreement. Controller confirms that Controller's instructions are exhaustively set out in the Agreement. In case Controller subsequently wants to modify its instructions, it shall primarily use the functions offered by the Services. If such functions would however not be sufficient for implementing such new instructions, Controller shall contact Processor in writing. If such new instructions exceed the scope of the Services provided under the Principal Agreement, Controller shall pay an additional reasonable remuneration for such additional Processor activities, based on the actually delivered work. Instructions must be reasonable, compliant with Data Protection Laws and consistent with the Principal Agreement.

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 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 purposes of the Principal Agreement, and to comply with Data Protection Laws in the context of that individual's duties to the 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 General authorization. Controller gives its general authorization to allow Processor to involve Processor's affiliated companies and other subcontractors as Sub-processors to process Controller Personal Data in connection with the provision of the Services, to the extent such appointment does not lead to non-compliance with any applicable law or Processor's obligations under this Agreement. Processor ensures that the involved Sub-processors are properly qualified, will be under an agreement with Processor and comply with data processing obligations similar to the ones which apply to Processor under this Agreement. Processor regularly monitors the performance of its Sub-processors and is liable for their work towards the Controller.

5.2 Change of Sub-processor. Processor is free to choose and change Sub-processors. Upon request, Processor shall inform Controller of the main Sub-processors currently involved. In case there is a later change of any main Sub-processor (addition or replacement), Processor shall notify Controller of such change. Should the processing be subject to the GDPR EU and/or GDPR UK and should Controller reasonably demonstrate that such new Sub-processor has breached, or is likely to breach, the GDPR EU and/or GDPR UK and therefore not be able to support the involvement of that new Sub-processor, Processor will undertake reasonable efforts to remedy this situation. Should this not be remedied and Processor continues to involve the related new Sub-processor for the Services, Controller shall be entitled to terminate the related part(s) of the Principal Agreement for which the related new Sub-processor is involved, subject to three (3) months' prior notice, without any compensation or exit penalty being due by Processor. To avoid any misunderstanding, should Controller not exercise this right of termination, it shall be deemed to support the involvement of the related Sub-processor and Processor confirms to continue to be liable for this Sub-processor's work towards Controller, in accordance with clause 5.1.

In accordance with clause 5.2 above, details of current Sub-processors who will have access to The Controller Personal Data are specified in **Annex III** of this Agreement

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 the Controller 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 as far as they apply to its operations.

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 Data Protection Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by applicable law, inform Controller of that legal requirement before the Processor responds to the request.

6.4 Controller shall pay an additional reasonable remuneration to Processor for handling such assistance requests.

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 reasonably co-operate with he Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation and mitigation of each such Personal Data Breach. To the extent the Personal Data Breach results from Processor's breach of the Agreement, Processor will use commercially reasonable efforts to remediate the cause of 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 and,
V. 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 Processors.

8.2 Controller shall pay an additional reasonable remuneration to Processor for handling such assistance requests.

9. Deletion or return of The Controller Personal Data

9.1 Subject to this section 9, Processor shall within reasonable time 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 The Controller Personal Data, except to the extent that Processor is under a statutory obligation to continue storing such Controller Personal Data.

9.2 Upon Company's request, Processor shall provide written certification to Company that it has fully complied with this section 9

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to The Controller on request all existing documentation necessary to demonstrate compliance with this Agreement, free of charge.

10.2 For any additional documentation, support or service requested by Controller, reserves the right to invoice the Controller all reasonable costs directly arising from such Controller requests. This shall also include adequate compensation for the working hours of Processor staff while they are supporting Controller's audit, unless as far as the audit reveals that Processor does not comply with its obligations under this Agreement.

10.3 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

To provide the Services, Controller accepts that Processor may have Personal Data processed and accessible by its Sub-processors (as defined in clause 5.1) outside Controller's country of domicile. In case the processing is subject to the GDPR EU and Controller Personal Data is transferred from the European Economic Area ("EEA") to a Sub-processor for processing in any country outside the EEA that is not recognized by the European Commission as providing an adequate level of protection for personal data, appropriate safeguards are provided by Standard Contractual Clauses with the non-EEA Sub-processor, as specified in the Data Transfer Addendum II to the Initial Agreement, or by any other appropriate safeguard as foreseen under the GDPR EU. In case the processing is subject to the GDPR UK and Personal Data is transferred from the UK to a Sub-processor for processing in any country outside the UK that is not recognized by the UK Government as providing an adequate level of protection for personal data, appropriate safeguards are provided as foreseen under the GDPR UK.

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

This Agreement is subject to the Principal Agreement, to which it is added as Addendum I. In case of conflict between this Agreement and Addendum II, the provisions of Addendum II shall prevail.

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

1. Data _Controller_ Company:

Signature:_____

Name: _____

Title:_____

Date:_____

2. Data _Processor_ Company: Glantus

Signature: 

Name: John Robinson

Title: Group Compliance Manager and DPO

ANNEX I: DESCRIPTION OF PERSONAL DATA PROCESSING

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

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

Processor shall process Controller Personal Data to provide the Services set forth in the Principle Agreement. Processor's processing of Controller Personal Data shall terminate upon the destruction or return of Controller Personal Data. Data is only held for the duration of an active Principle Agreement.

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 obtained 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 Processor has implemented in accordance with Section 4 of this Agreement and Data Protection Laws.

Processor information below:

Glantus implement appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Controller 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 Processor is Processing Company Personal Data and in accordance with the requirements of all Data Protection Laws;

Use encryption methods to safeguard Controller 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 Controller 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.

Glantus uses Microsoft Azure platform for EU/UK and US data. Data is segregated per jurisdiction, this is achieved by hosting dedicated data stores in the country where the data originates. Microsoft Azure hold an equivalent high standard in data protection compliance and cyber security to Glantus. For more information please visit Azure compliance documentation | Microsoft Docs.

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.

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

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.

JIRA – Atlassian – Technical support – Retention is governed by subject access request under CCPA, Massachusetts Data Protection Law and local Data Protection legislation. Data is retained for operational purposes.

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

Azure (EU) – Microsoft – Cloud Storage – Retention for duration of project.

US Data Centre (US data only) – TierPoint – Retention for as long as customer contact is active.