DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "***DPA***") forms part of that certain Kiteworks Solution License Agreement (the "***Agreement***") effective as of the latest date of its execution by and between_____________________________ (the "***Customer***") and Kiteworks USA, LLC (together with its affiliated companies, "***Kiteworks***"). It is entered into for compliance with the General Data Protection Regulation (EU) 2016/679 (the "***GDPR***").

1. Definitions: Scope.

1.1 Definitions.

(a) Unless otherwise defined herein, capitalized terms in this DPA shall have the meanings ascribed to them in the Agreement.

(b) "***Data Protection Legislation***" means all applicable legislation relating to data protection and privacy including without limitation the CCPA the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., as updated, amended or replaced from time to time.("***California Privacy Law***"), General Data Protection 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 ("***GDPR***"), the United Kingdom Act of Parliament of 23 May 2018 as updated by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 laid on 14 October 2020 ("***UK GDPR***"), together with any national implementing laws in any Member State of the European Union, the UK or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time.

(c) The terms "***controller***", "***data subject***", "***personal data***", "***personal data breach***", "***processing***", "***processor***", "***service provider***", "***consumer***", "***consumer personal information***" "***business purpose***", "***aggregate consumer information***", "***deidentified information***", "***sell***", and "***third party***" shall have the same meaning as in the Data Protection Legislation.

1.2 Scope. The provisions of this DPA prevail over the provisions of the Agreement with respect to personal data hosted by Kiteworks pursuant to the Agreement. If adjustments to this DPA are necessary to comply with legal requirements, the parties shall make such adjustments promptly. To the extent the laws of any jurisdiction within the EU are contrary to this DPA or require a modification tothis DPA, Customer shall have the responsibility of informing Kiteworks. Customer acknowledge and agrees that, with the exception of support services provided to Customer's Designated Users, the nature of the Kiteworks Solution (a) does not enable Kiteworks to have access to personal data processed via the

Kiteworks Solution and (b) the level of encryption applied to Customer Data via the Kiteworks Solution renders any personal data unintelligible to any person who is not authorized to access it, including but not limited to Kiteworks. Therefore, while the obligations set forth in this DPA apply to all personal data processed by Kiteworks, all obligations set forth herein requiring Kiteworks' access to such personal data shall not be applicable unless Kiteworks comes into possession of personal data that has not been rendered unintelligible by way of encryption or other methods.

1.3 Application of the Standard Contractual Clauses Document. If processing of personal data involves an international transfer, the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, as the case may be, apply, and are incorporated by reference as set forth in Appendix.

1.4 California Privacy Law. Accellion USA, LLC is a service provider for the purposes of the services it provides to Customer pursuant to the Agreement, according to the meaning given to that term in the California Privacy Law. Accellion USA, LLC agrees that, to the extent that Customer discloses a consumer's personal information to Accellion USA, LLC, Accellion s USA, LLC will process that personal information only on behalf of Customer pursuant to the Agreement and this DPA. Accellion USA, LLC certifies that it shall not process, retain, use or disclose a consumer's personal information for any purpose other than (i) for the specific purpose of providing the Kiteworks Solution or providing services, as applicable, pursuant to the Agreement; (ii) to create aggregate consumer information and/or deidentified information; and (iii) as otherwise permitted for a service provider under the California Privacy Law, including without limitation a business purpose. Accellion USA, LLC agrees that it shall not sell a consumer's personal information. Accellion USA, LLC certifies that it understands the restrictions set forth for service providers in the California Privacy Law and will comply with them.

1.5 Notice and Consent Regarding Transfer of Data. Use of the Kiteworks Solution requires that personal data be processed in: (i) the United States of America by Accellion USA, LLC if hosting is provided by Accellion USA, LLC in the United States of America, or if Customer's End Users utilize Kiteworks' mobile applications, or where Accellion USA, LLC provides customer support; (ii) Europe by Accellion UK Ltd and Accellion GmbH; and (iii) Singapore by Kiteworks Pte Ltd, where customer support teams are located. Computing systems, resources and infrastructure necessary for those functions and, hence, for Customer's exercise of its rights under the Agreement, are located in those jurisdictions. Those items would not be available without such processing of personal data in the United States of America, Europe, and Singapore as described. Pursuant to Article 49 of the GDPR, Customer hereby expressly consents to the processing by, and transfer of, personal data to Accellion USA, LLC in the United States of America, Accellion UK Ltd. and Accellion GmbH in Europe, and Kiteworks Pte Ltd in Singapore for those purposes. Kiteworks Pte Ltd, Accellion UK Ltd, and Accellion GmbH are subsidiaries of Accellion USA, LLC and each entity processes such personal data in compliance with the contractual requirements established with Customer.

2. Roles and Responsibilities.

2.1 Roles & Responsibilities.

(a) Customer as Controller. Customer represents that it is the sole controller of the personal data for the purposes of the GDPR and applicable Data Protection Legislation and has all necessary rights, and has obtain all necessary consents to use the personal data with the Kiteworks Solution. Customer has the right to give instructions regarding the nature, scope and process of personal data pursuant to express terms in the GDPR. Kiteworks will comply and maintain records for all such instructions to the extent necessary for Kiteworks to: (i) comply with its processor obligations under the GDPR and applicable Data Protection Legislation; or (ii) assist Customer to comply with Customer's obligations as a controller under the GDPR or applicable Data Protection Legislation relevant to Customer's use of the Kiteworks Solution. Customer represents and warrants that is responsible for the lawfulness of the processing of the personal data usingthe Kiteworks Solution and Customer agrees that it will not use the Kiteworks Solution in conjunction withpersonal data to the extent that doing so would violate the GDPR or applicable Data Protection Legislation. Customer further represents and warrants that personal data used with the Kiteworks Solution will not subject Kiteworks to any obligations beyond those set forth in the Agreement, the DPA or any other writtenagreement between the parties.

(b) Kiteworks as Processor. Kiteworks is the processor and processes personal data solely for the purposes mentioned in the Agreement on behalf of Customer's instructions as embodied in the Agreement. Kiteworks shall not use the personal data for any other purpose. Kiteworks will monitor itscompliance with data protection requirements and its contractual obligations as well as the documented and authorized instructions of Customer provided during the term of the Agreement. To the extent required by the GDPR or applicable Data Protection Legislation, Kiteworks will immediately inform Customer if, in its opinion, Customer's instructions violate the GDPR or applicable Data Protection Legislation, but Customer acknowledges and agrees thatKiteworks is not responsible for performing legal research and/or for providing legal advice to Customer.Kiteworks shall create records of all processing activities in its responsibility meeting at least the requirements of Article 30(2) and (3) of the GDPR.

2.2 Limitations. Customer acknowledges and agrees that software and services provided by Kiteworks give the Customer, not Kiteworks, control over access, additions, deletions, modifications, and monitoring of personal data and that, accordingly: (i) the core activities of Kiteworks do not involve any monitoring of a data subject; and (ii) Kiteworks does not have actual knowledge of the types of personal data that Customer may host using the Kiteworks Solution. Hence, Kiteworks does not have to appoint a dataprotection officer as referenced in Article 37 of the GDPR or a representative in the EU pursuant to Article27(2)(a) of the GDPR.

2.3 Sub-processors. Customer and Data Controllers authorize Kiteworks to subcontract the processing of personal data to sub-processors. Kiteworks is responsible for any breaches of the Agreement caused by its sub-processors. Sub-processors will have the same obligations in relation to Kiteworks as Kiteworks does as a Data Processor (or sub-processor) regarding their processing of personal data. Kiteworks will evaluate the security, privacy, and confidentiality practices of a subprocessor prior to selection. Sub-processors may have security certifications that evidence their use of appropriate security measures. If not, Kiteworks will regularly evaluate each sub-processor's security practices as they relate to data handling.

2.4 New sub-processors. Kiteworks' use of sub-processors is at its discretion, provided that:

(a) Kiteworks will notify Customer in advance (by email or such other means which Kiteworks makes available to its customers) of any changes to the list of sub-processors in place on the Effective Date (except for Emergency Replacements or deletions of sub-processors without replacement).

(b) If Customer has a legitimate reason that relates to the sub-processors' processing of personal data, Customer may object to Kiteworks' use of a sub-processor, by notifying Kiteworks in writing within thirty days after receipt of Kiteworks' notice. If Customer objects to the use of the subprocessor, the parties will come together in good faith to discuss a resolution. Kiteworks may choose to: (i) not use the subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new subprocessor.

(c) If Customer's objection remains unresolved sixty days after it was raised, and Kiteworks has not received any notice of termination, Customer is deemed to accept the subprocessor.

(d) The list of sub-processors current as of the Effective Date shall be set forth in Appendix 1.

2.5 Emergency Replacement. Kiteworks may change a subprocessor where the reason for the change is outside of Kiteworks' reasonable control. In this case, Kiteworks will inform Customer of the replacement subprocessor as soon as possible. Customer retains its right to object to a replacement subprocessor under Section 2.4.

3. Technical and Organizational Measures. As set forth in Appendix 2, Kiteworks takes appropriate technical andorganizational measures for its own systems to comply with data privacy in order to ensure a level of dataprotection appropriate to the risk resulting from the processing of personal data under the Agreement, 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 severity and likelihood of realization of risks for the rights and freedoms of data subjects. In particular, Kiteworks offers versions of the Kiteworks Solution which are certified as FIPS 140 compliant and/or for which Kiteworks has received FedRAMP authorization.

4. Personal Data; Audit.

4.1 Rights in Personal Data. Kiteworks recognizes that the right to use personal data is exclusive to Customer as data controller and Kiteworks does not claim any rights over the personal data. To the extent permitted by law, Kiteworks will inform Customer of requests made directly to Kiteworks from data subjects exercising their rights regarding personal data. Since it is the Customer, not Kiteworks, which retains control over the access, additions, deletions, modifications and monitoring of personal data, Customer shall be responsible to respond to such requests of data subjects. Similarly, if Kiteworks receives any subpoena or similar order from a court or other governmental authority which relates to the processing of personal data on behalf of the Customer, it will promptly pass on the same to Customer without responding to it, unless otherwise required by applicable law, and Customer shall promptly respond to the same. Upon termination or expiration of the Agreement, to the extent that Kiteworks maintainsany personal data of Customer, it will either delete or return such personal data unless otherwise requiredby applicable law.

4.3 Reporting of Unauthorized Access. Kiteworks shall inform the Customer without undue delay, but at least within 48 hours, about any errors or unauthorized access or disclosure in processing of personal data of theCustomer or any other breach of the protection of personal data.

4.4 Audit. At its sole cost and expense, Customer may audit Kiteworks' compliance with its obligations under this DPA up to once per year and upon at least 14 days advance written notice to Kiteworks, with such notice to include a detailed proposed audit plan; provided that to the extent required by the GDPR or applicable Data Protection Legislation, Customer or the relevant data protection authority may perform more frequent audits. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Kiteworks will review the proposed audit plan and provide Customer with any concerns or questions and work cooperatively with Customer to agree on a final audit plan. Kiteworks will contributeto such audits by providing the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to Customer's use of the Kiteworks Solution where such records are not otherwise available to the Customer through the Kiteworks Solution.The audit must be conducted during regular business hours, may not unreasonably interfere with Kiteworksbusiness activities, and be conducted subject to the agreed final audit plan and Kiteworks' or the applicable sub processor's internal policies. Customer will provide Kiteworks any audit reports generatedas part of any audit under paragraph unless prohibited by the GDPR, applicable Data Protection Legislation, or the applicable data protection authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of the parties under the terms of the Agreement. Where assistance requested of Kiteworks in conjunction with such audit requires the use of resources different from or in addition to those required of Kiteworks under the Agreement, Customer shall pay for such additional resources at Kiteworks' then-current rates.

5. Liabilities. Liability of the parties under this DPA is governed by the Agreement.

IN WITNESS WHEREOF, the Parties hereto, through their duly authorized representatives, have executed this Agreement as of the Effective Date.

KITEWORKS: **CUSTOMER:** _________________

By:_____________________________

Name:__________________________

Title:___________________________

Date:___________________________

By: ____________________________

Name: __________________________

Title: ___________________________

Date: ___________________________

Appendix List

Appendix 1 – Details of Data Processing

Appendix 2 – Technical and Organizational Measures

Appendix 3 – Standard Contractual Clauses

Appendix 1

Details of Data Processing

Data Exporter

Name: The Customer or other Data Controller subscribed to the Kiteworks Solution that allows authorized users to enter, amend, use, delete or otherwise process personal data, as identified in the Agreement.

Address: As stated in the Agreement.

Contact person's name, position and contact details: _______________

Representative in the EU/UK, as applicable: _______________

Role: (Controller/Processor): Controller

Data Importer

Name: Kiteworks and its sub-processors, each as identified in the Agreement.

Address: As stated in the Agreement.

Contact person's name, position and contact details: Mehreen Mir, Sr. Contracts Manager, privacy@kiteworks.com

Data protection officer: N/A

Representative in the EU/UK, as applicable: Privacy inquiries should be directed to privacy@kiteworks.com.

Role: (Controller/Processor): Processor

Purpose(s) of the data transfer and further processing

Provision by Kiteworks of the Kiteworks Solution that includes the following support: *customer support to end users of the Kiteworks Solution*

Description of Transfer

Kiteworks is the processor and processes personal data solely for the purposes mentioned in the Agreement on behalf of Customer's instructions as embodied inthe Agreement. Kiteworks shall not use the personal data for any other purpose. Kiteworks will monitor itscompliance with data protection requirements and its contractual obligations as well as the documented and authorized instructions of Customer provided during the term of the Agreement.

Categories of Data Subjects whose personal data is transferred

End users of the Kiteworks Solution.

Categories of personal data transferred

The transferred personal data submitted into the Kiteworks Solution may concern the following categories of data:

Personal Identifiable Information (PII) (First Last Names, Telephone number, email 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. *N/A*

Processing Operations (Activities relevant to the data transferred under the DPA)

The transferred personal data is subject to the following basic processing activities:

The nature of the processing may include, but is not limited to, collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *For the duration of the License Agreement.*

Competent supervisory authority: *Netherlands.*

Adequacy decisions and/or appropriate safeguards

The following adequacy decisions and/or appropriate safeguards will apply to this Processing: Not applicable.

List of Subcontractors as of the Effective Date

Company	Purpose	Hosting location
Amazon Web Services, Inc.	Cloud service provider	United States
Salesforce Inc.	CRM solution	United States

Appendix 2

Technical and Organizational Measures

The following sections define the Kiteworks' current technical and organizational security measures. Kiteworks may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

Control		**Data Importer's response:**
Physical access control	Description of measures to prevent unauthorized third parties from accessing data processing systems (DP systems) that allow the processing or use of personal data.	Customer data is managed and owned by customer through Bring Your Own Key (BYOK). Data is protected at AES-256 at rest and only accessible by customer with appropriate decryption key.
Access control	Description of measures to prevent unauthorized third parties from using data processing systems that allow the processing or use of personal data.	Customer data is managed and owned by customer through Bring Your Own Key (BYOK). Data is protected at AES-256 at rest and only accessible by customer with appropriate decryption key.
User access control	Description of measures to prevent persons from accessing data that is not considered mandatory in order to fulfil their tasks.	Customer data is managed and owned by customer through Bring Your Own Key (BYOK). Data is protected at AES-256 at rest and only accessible by customer with appropriate decryption key.
Transmission control	Description of measures to prevent unauthorized third parties from accessing personal data during transmission and/or transport.	Customer data is managed and owned by customer through Bring Your Own Key (BYOK). Data is protected at AES-256 at rest and only accessible by customer with appropriate decryption key.

Entry control	Description of measures to ensure consistent tracking if personal data has been entered, amended or removed from data processing systems and by whom.	Kiteworks platform performs a full audit trail of data imported into the customer data. Data is tracked throughout its entire lifecycle through deletion.
Order control	Description of measures to ensure that personal data can only be processed in accordance with the instructions issued by the client.	Customer data is managed and owned by customer through Bring Your Own Key (BYOK). Data is protected at AES-256 at rest and only accessible by customer with appropriate decryption key. PII of customer is only used to provide customer support and notifications. Customer may request removal of data at contract termination. PII used for services will be archived within 60 days
Availability control	Description of measures to protect personal data against accidental destruction or loss.	All customer data hosted in AWS is backed up every 72 hours, retaining the last 2 backups. Customer may also choose additional High Availability options through multi-node deployments across multiple regions offered by AWS.
Separation rule	Description of measures to ensure separate processing of different data sets.	All hosted customers are assigned unique Virtual Private Cloud (VPC) within AWS. Data separation is logically separated, with physical separation inherited from AWS.

Appendix 3

STANDARD CONTRACTUAL CLAUSES

1. EU Standard Contractual Clauses

EU SCC term	Amendment / Selected option
Module	Module 2 (Controller to Processor)
Clause 7 (Docking clause)	not included
Clause 9 (Use of sub-processors) / Annex III	Option 2 shall apply. The list of sub-processors already authorized by Customers is contained in Appendix 1.
Clause 11 (Redress)	not included
Clause 13 (Supervision) and Annex 1.C	The supervisory authority with responsibility for ensuring compliance by the data exporter is: where the data exporter is established within an EU member state, the supervisory authority of that EU member state **OR** where the data exporter is subject to EU GDPR pursuant to Article 3(2) EU GDPR and has appointed a representative in [Note to supplier: where applicable, *insert country where representative is established*, the supervisory authority of that EU member state **OR** where the data exporter is subject to EU GDPR pursuant to Article 3(2) EU GDPR, but has not appointed a representative in an EU member state, the supervisory authority of the EU member state where the relevant data subjects are located.
Clause 17 (Governing law)	Laws of the Netherlands
Clause 18 (Choice of forum and jurisdiction)	Courts of the Netherlands

Annex I.A (List of parties)	The relevant data exporters and data importers are specified in Appendix 1.
Annex I.B (Description of the transfer)	The categories of data subject, personal data categories, purposes of international transfer and processing, any additional safeguards, and if applicable the duration of processing and any maximum data retention periods are specified in Appendix 1.
Annex II (Technical and organizational measures)	The relevant technical and organizational measures are specified in Appendix 2.

2. UK Standard Contractual Clauses

2.1 UK Data Transfer Addendum

UK Data Transfer Addendum *Incorporating EU Standard Contractual Clause terms*	**Amendment / Selected Option**
Clause 7 (Docking clause)	not included
Clause 9 (Use of sub-processors) / Annex III	Option 2 shall apply. The list of sub-processors already authorized by Customer is contained in Appendix 1.
Clause 11 (Redress)	not included
Clause 13 (Supervision) and Annex 1.C:	The competent supervisory authority is the UK Information Commissioner's Office.
Clause 17 (Governing law):	Laws of England
Clause 18 (Choice of forum and jurisdiction):	Courts of England and Wales
Clause 9	Clause 9 shall be amended to read: "The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England".
Annex I.A (List of parties)	The relevant data exporters and data importers are specified in Appendix 1.
Annex I.B (Description of the transfer)	The categories of data subject, personal data

	categories, purposes of international transfer and processing, any additional safeguards, and if applicable the duration of processing and any maximum data retention periods are specified in Appendix 1.
Annex II (Technical and organizational measures)	The relevant technical and organizational measures are specified in Appendix 2.

2.2 UK Controller-Processor Standard Contractual Clauses

UK Controller-Processor SCC (2010/87/EU)_	**Amendment / Selected Option**
Appendix 1	Appendix 1 identifies: 1.1 the "data exporter(s)”. 1.2 the "data importers(s)”. 1.3 the categories of data subject whose personal data is transferred. 1.4 the categories of personal data transferred (including special category data). 1.5 the activities of each of the "data importer(s)" and "data exporter(s)" and the purposes for which each uses the personal data being transferred. 1.6 the processing operations to which the Customer personal data transferred will be subject
Appendix 2	Appendix 2 identifies the relevant technical and organizational measures.
Clause 9 (Governing law)	Clause 9 shall be amended to read: "The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England".