Accellion

DATA PROCESSOR ADDENDUM

This Data Processor Addendum (the "***DPA***") forms part of that certain Accellion Solutions License Agreement (the "***Agreement***") dated_____by and between_____(the "***Customer***") and Accellion USA, LLC (together with its affiliated companies, "***Accellion***"). It is entered into for compliance with the General Data Protection Regulation (EU) 2016/679 (the "***GDPR***").

1. Definitions: Scope.

1.1 Definitions. Unless otherwise defined herein, capitalized terms in this DPA shall have the meanings ascribed to them in the Agreement. The terms "***controller***", "***data subject***", "***personal data***", "***personal data breach***", "***processing***" and "***processor***" shall have the same meaning as in the GDPR.

1.2 Scope. The provisions of this DPA prevail over the provisions of the Agreement with respect to personal data hosted by Accellion 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 Accellion. Customer acknowledge and agrees that, with the exception of support services provided to Customer's Designated Users, the nature of the Accellion Solution (a) does not enable Accellion to have access to personal data processed via the Accellion Solution and (b) the level of encryption applied to Customer Data via the Accellion Solution renders any personal data unintelligible to any person who is not authorized to access it, including but not limited to Accellion. Therefore, while the obligations set forth in this DPA apply to all personal data processed by Accellion, all obligations set forth herein requiring Accellion's access to such personal data shall not be applicable unless Accellion 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 Notice and Consent Regarding Transfer of Data. Use of the Accellion 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 Accellion's mobile applications, or where Accellion USA, LLC provides customer support; (ii) Europe by Accellion UK Ltd and Accellion GmbH; and (iii) Singapore by Accellion 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 Accellion Pte Ltd in Singapore for those purposes. Accellion 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 laws and has all necessary rights, and has obtain all necessary consents to use the personal data with the Accellion Solution. Customer has the right to give instructions regarding the nature, scope and process of personal data pursuant to express terms in the GDPR. Accellion will comply and maintain records for all such instructions to the extent necessary for Accellion to: (i) comply with its processor obligations under the GDPR and applicable law; or (ii) assist Customer to comply with Customer's obligations as a controller under the GDPR or applicable law relevant to Customer's use of the Accellion Solution. Customer represents and warrants that is responsible for the lawfulness of the processing of the personal data usingthe Accellion Solution and Customer agrees that it will not use the Accellion Solution in conjunction withpersonal data to the extent that doing so would violate the GDPR or applicable data protection laws. Customer further represents and warrants that personal data used with the Accellion Solution will not subject Accellion to any obligations beyond those set forth in the Agreement, the DPA or any other writtenagreement between the parties.

(b) Accellion as Processor. Accellion 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. Accellion shall not use the personal data for any other purpose. Accellion will monitor its compliance 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 law, Accellion will immediately inform Customer if, in its opinion, Customer's instructions violate the GDPR or applicable law, but Customer acknowledges and agrees that Accellion is not responsible for performing legal research and/or for providing legal advice to Customer. Accellion 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 Accellion give the Customer, not Accellion, control over access, additions, deletions, modifications and monitoring of personal data and that, accordingly: (i) the core activities of Accellion do not involve any monitoring of a data subject; and (ii) Accellion does not have actual knowledge of the types of personal data that Customer may host using the Accellion Solution. Hence, the provisions of Article 11 of the GDPR apply to the processing conducted by Accellion; and (iii) Accellion does not have to appoint a data protection officer as referenced in Article 37 of the GDPR or a representative in the EU pursuant to Article 27(2)(a) of the GDPR.

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

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

(a) Accellion will notify Customer in advance (by email or such other means which Accellion 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 Accellion's use of a sub-processors, by notifying Accellion in writing within thirty days after receipt of Accellion's notice. If Customer objects to the use of the sub-processors, the parties will come together in good faith to discuss a resolution. Accellion may choose to: (i) not use the sub-processors or (ii) take the corrective steps requested by Customer in its objection and use the sub-processors. 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 sub-processors.

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

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

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

3. Technical and Organizational Measures. As set forth in Appendix 2, Accellion 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, Accellion offers versions of the Accellion Solution which are certified as FIPS 140 compliant and/or for which Accellion has received FedRAMP authorization.

4. Personal Data; Audit.

4.1 Rights in Personal Data. Accellion recognizes that the right to use personal data is exclusive to Customer as data controller and Accellion does not claim any rights over the personal data. To the extent permitted by law, Accellion will inform Customer of requests made directly to Accellion from data subjects exercising their rights regarding personal data. Since it is the Customer, not Accellion, 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 Accellion 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 Accellion 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. Accellion 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 the Customer or any other breach of the protection of personal data.

4.4 Audit. At its sole cost and expense, Customer may audit Accellion's compliance with its obligations under this DPA up to once per year and upon at least 14 days advance written notice to Accellion, with such notice to include a detailed proposed audit plan; provided that to the extent required by the GDPR or applicable law, 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. Accellion 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. Accellion 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 Accellion Solution where such records are not otherwise available to the Customer through the Accellion Solution.The audit must be conducted during regular business hours, may not unreasonably interfere with Accellion business activities, and be conducted subject to the agreed final audit plan and Accellion's or the applicable sub processor's internal policies. Customer will provide Accellion any audit reports generatedas part of any audit under paragraph unless prohibited by the GDPR, applicable law, 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 Accellion in conjunction with such audit requires the use of resources different from or in addition to those required of Accellion under the Agreement, Customer shall pay for such additional resources at Accellion's 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.

ACCELLION: _____	**CUSTOMER:** _____
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	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 Accellion 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: *[INSERT]*

Representative in the EU/UK, as applicable: *[INSERT]*

Role: (Controller/Processor): *Controller*

Data Importer

Name: *Accellion and its sub-processors, each as identified in the Agreement or this DPA.*

Address: *As stated in the Agreement*

Contact person's name, position and contact details: *privacy@kiteworks.com*

Data protection officer: *Privacy inquiries should be directed to privacy@kiteworks.com.*

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

Role: (Controller/Processor): *Processor*

Purpose(s) of the data transfer and further processing

Provision by Accellion of the Accellion Solution that includes the following support: *Technical/Customer support to the end user(s) of Accellion Solution.*

Description of Transfer

Accellion 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. Accellion shall not use the personal data for any other purpose. Accellion 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 Accellion Solution

Categories of personal data transferred

The transferred personal data submitted into the Accellion Solution may concern the following categories of data: *Personal Identifiable Information (PII)*

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: *collection, storage, erasure/destruction.*

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

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *Thirty (30) days*

Competent supervisory authority: *The 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**

Appendix 2

Technical and Organizational Measures

The following sections define the Accellion's current technical and organizational security measures. Accellion 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 unauthorised 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 unauthorised 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 unauthorised 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 of contract end.
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 organisational 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 authorised 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".