Wripple™ Data Protection Addendum

This Data Processing Addendum ("**DPA**") supplements and amends the terms and forms part of the Agreement (as defined below) by and between the customer identified in the Agreement and/or Order From (the "**Customer**" or "**you**" or "**your**") and the applicable Unisoft International, Inc., dba SMA Technologies entity providing the SMA Offering product and services Offerings ("**SMA Technologies**", "**we**", "**us**", or "**our**").

1. DEFINITIONS

The following capitalized terms have the indicated definitions and meanings:

"Account Data" means information about Customer that Customer provides to SMA Technologies in connection with the creation or administration of its SMA Technologies accounts, such as first and last name, username, and email address of a User or Customer's billing contact.

"**Affiliate**" means an entity that controls, is directly or indirectly controlled by or is under common control of the relevant party.

"Agreement" means the written contract, Order Form, and if applicable, Statement of Work, in place between Customer and SMA Technologies in connection with the purchase of SMA Offerings by Customer.

"**Applicable Laws**" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, ordinances and other pronouncements having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority.

"Breach" means any confirmed breach of the Security Measures resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by SMA Technologies or its Subprocessors.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data, including as applicable any "business" as that term is defined by the CCPA.

"**Customer**" has the meaning assigned to that term in the Agreement.

"**Customer Content**" means data provided by Customer for processing via the Services including, without limitation, the contents of the files, Personal Data, emails, or messages sent by or to a permitted user.

"**Data Protection Law**" means all Applicable Laws that govern the Processing of Personal Data, which may include, but is not limited to, any applicable local, state, federal and foreign privacy, cybersecurity and breach notification laws and regulations; the California Consumer Privacy Act of 2018, as modified by the California Privacy Rights Act of 2020 ("CPRA"); the Virginia Consumer Data Protection Act ("VaCDPA"); the Colorado Privacy Act ("CPA"); the Utah Consumer Privacy Act ("UCPA");the Connecticut Data Privacy Act ("CTDPA"); Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"); the United Kingdom ("**UK**") Data Protection Act 2018 and the UK General Data Protection Regulation ("**UK GDPR**"); Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and (v) any relevant law, statute, regulation, legislative enactment, order or other binding instrument that implements or amends the foregoing..

"**Data Subject**" means (i) "data subject" as defined under the GDPR, (ii) "consumer" or "household" as defined under the CCPA, and/or (iii) such similar term under the relevant Data Protection Law.

"**Data Subject Request**" refers to a request from (i) a Data Subject in accordance with the GDPR and/or the CCPA and/or (ii) such similar term under the relevant Data Protection Law.

"**GLBA**" means the federal Gramm-Leach-Bliley Act and its implementing regulations, including Regulation P.

"**GLBA Information**" refers to any nonpublic personal information (as that term is defined in the GLBA) that is collected, processed, sold or disclosed by or to a Party subject to the GLBA.

"**Personal Data**" means (i) means any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular natural person, (ii) "personal data" as defined under the GDPR, (ii) "personal information" as defined under CCPA, and/or (iii) such similar term under the relevant Data Protection Law, that is under the control of Customer and Processed by SMA Technologies in connection with the performance or provision of the SMA Offering. For the purpose of this Addendum, the term Personal Data does not include any GLBA Information.

"**Process**", "**Processed**" or "**Processing**" means "processing" as defined under the relevant Data Protection Law, the details of which are outlined in Appendix A.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**Regulator**" means the data protection supervisory authority or other governmental or legal authority which has jurisdiction over the Processing of Personal Data.

"**SMA Offerings**" means the SMA Wripple™ product and services provided by SMA Technologies as identified in the Agreement and described further in an ordering document referencing the Agreement.

"**Subprocessor**" means any Processor engaged by SMA Technologies or our Affiliates.

"**Third Party**" means any person (including companies, entities, organizations, etc.) that is not Customer or SMA Technologies.

"**User**" means the Customer or any employee, consultant, or similar of the Customer that directly or indirectly has access and uses the SMA Offering.

All other capitalized terms not defined herein will have the meanings ascribed to them in the Agreement.

2. **PERSONAL DATA PROCESSING.**

2.1 **Scope.** This DPA reflects the parties' understanding regarding the Processing of Customer's Personal Data as part of our providing the SMA Offerings to you under the Agreement. Each party is responsible for its compliance with Data Protection Law as applicable to such party and for fulfilling any of its related obligations to third parties, including Data Subjects and Regulators**.**

2.2 **Parties Roles.** Customer and SMA Technologies agree that, as between the parties and except as to Account Data (for which Customer and SMA Technologies are independent Controllers), Customer is a Controller and SMA Technologies is a Processor of Personal Data.

2.3 **SMA Technologies as Processor.**

2.3.1 Generally. SMA Technologies shall Process Personal Data only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order(s); (ii) Processing initiated by Users in their use of the SMA Offerings

Services; and (iii) other reasonable instructions as may be additionally communicated in writing by Customer to SMA Technologies from time-to-time that are consistent with the terms of the Agreement. SMA Technologies shall inform you immediately (i) if we believe that an instruction from Customer constitutes a breach of the GDPR and/or (ii) if we are unable to follow Customer's instructions for the Processing of Personal Data. Pending the decision on the withdrawal, amendment, or confirmation of the relevant instruction, we shall be entitled to suspend the implementation of the relevant instruction.

2.3.2 SMA Technologies Personnel. We shall ensure that all persons authorized to Process Personal Data and are made aware of the confidential nature of the Personal Data and have committed themselves to maintain such confidentiality (*e.g.,* by confidentiality agreements) or are under an appropriate statutory obligation of confidentiality.

2.3.3 Personal Data Retention. Following the completion of the SMA Offerings, at Customer's choice, we shall either return to you or delete all Personal Data in our possession; *provided, however,* we may retain Personal Data to the extent the return or destruction of such Personal Data is impracticable or incidentally prohibited by applicable law or other valid legal process (*e.g.,* court order), and in such instances, we shall take measures to inform you and block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by applicable law) and shall continue to appropriately protect the Personal Data remaining in our possession.

2.4 **Customer as Controller.** Customer is solely responsible for ensuring that (i) the Personal Data submitted to us for Processing is duly authorized, with all necessary notices, rights, permissions, and consents (to include effective opt-out options); (ii) your instructions to us comply with Data Protection Laws and are consistent with the Agreement; and (iii) no special categories of Personal Data (*e.g.,* under GDPR Article 9) are submitted to us for Processing. For clarity, SMA Technologies does not – nor are we obligated to – assess the type or substance of Customer Content to identify whether it is Personal Data and/or subject to any specific legal requirements.

3. **DATA SUBJECT REQUESTS.** We shall, to the extent legally permitted, promptly notify you of any complaint, dispute, or request we receive from a Data Subject, including any Data Subject Request. We shall not respond to a Data Subject Request, except that you authorize us to redirect the Data Subject Request as necessary to allow you to respond directly. Taking into account the nature of the Processing, we shall assist you by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of you obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent you, in your use of the SMA Offerings, do not have the ability to address a Data Subject Request, we shall upon your request provide commercially reasonable efforts to assist you in responding to such Data Subject Request, to the extent we are legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, you are responsible for any costs arising from our provision of such assistance.

4. **SUBPROCESSORS.**

4.1 **Appointment.** We shall, by way of contract or other legal act, impose on each Subprocessor the equivalent data protection obligations as set out in this DPA. Customer authorizes our Affiliates to function as Subprocessors and to use any identified Subprocessors subject to the terms and conditions of this Section 4.

4.2 **Current Subprocessors; Notification of New Subprocessors.** Our Subprocessors will be identified at Appendix C and may be updated by us from time to time in accordance with this DPA. We will provide you with prior written notice of new Subprocessor appointments using the notice provisions

in the Agreement or through an alert in a User interface in the SMA Offerings; *provided, however*, that we will notify you in writing without undue delay after the appointment of a new, temporary Subprocessor if direct involvement of such Subprocessor is necessary for maintaining the availability and security of the SMA Offerings or Customer Content.

4.3 **Objection Right for New Subprocessors.** You may object to a new Subprocessor on a reasonable basis related to the Processing of Personal Data by notifying us in writing within fifteen (15) days after receiving an appointment notice; otherwise, we will deem the appointment of the new Subprocessor authorized by you. Upon receipt of an objection notice from you, we will use reasonable efforts to make available to you a change in the SMA Offerings or recommend a commercially reasonable configuration or use of the SMA Offerings to avoid the Processing of Personal Data by the new Subprocessor. If we cannot address your objection pursuant to the foregoing efforts, we will notify you of such and you may then terminate this DPA and any affected SMA Offering and receive a refund of prepaid fees covering the terminated portion of the applicable SMA Offering effective on thirty (30) days' written notice from the receipt of our notice to you.

4.4 **Liability.** We shall be liability for the acts and omissions of our Subprocessors to the same extent we would be liable if performing the services of each Subprocessor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

5. **SECURITY.**

5.1 **Security Measures.** SMA Technologies will implement and maintain the Security Measures detailed in Appendix 2 to this DPA. Customer acknowledges that the Security Measures are subject to technical progress and development and that SMA Technologies may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the SMA Offering. Notwithstanding the foregoing, Customer is solely responsible for independently assessing and implementing such security configuration settings made available to Customer by SMA Technologies as Customer deems necessary to meet your requirements and legal obligations under applicable Data Protection Laws. Customer acknowledges that, through its Users, Customer: (i) controls the type and substance of Customer Content; and (ii) sets User permissions to access Customer Content (to include Access Credentials); and therefore, Customer is responsible for reviewing and evaluating whether the documented functionality of an SMA Offering meets Customer's required security obligations relating to Personal Data under Data Protection Laws.

5.2 **Demonstration of Compliance.** We will make all information reasonably necessary to demonstrate compliance with this DPA available to you, including responses to information security and audit questionnaires. To the extent the Standard Contractual Clauses apply and the Customer reasonably argues and establishes that the above documentation is not sufficient to demonstrate compliance with the obligations laid down in this DPA, the Customer may execute an audit as outlined under Clause 8.9 of the Standard Contractual Clauses accordingly, provided that in such an event, the parties agree that any audit will be: (i) limited to Processing and storage facilities operated by SMA Technologies or any of our Affiliates, and be proportional to the nature and complexity of the SMA Offerings used by Customer; (ii) performed no more than one time per contract year on at least three (3) weeks' advance written notice to SMA Technologies (unless a shorter period is required for emergent circumstances (*e.g.,* Breach) during SMA Technologies' ordinary business hours; and (iii) conducted according to mutually agreed upon conditions as to the scope, timing, and duration of the audit and the reimbursement rate, if any, Customer is responsible for as to SMA Technologies' time expended in connection with such audit.

Customer will promptly provide SMA Technologies with information regarding any non-compliance discovered during an audit.

5.3 **Data Protection Impact Assessment.** Upon your request, we shall provide you with reasonable cooperation and assistance needed to fulfill your obligations under Data Protection Laws to carry out a data protection impact assessment related to your use of the SMA Offerings, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to SMA Technologies.

6. **BREACH MANAGEMENT AND NOTIFICATION.** We maintain industry-recognized security incident management policies and procedures and shall notify you without undue delay after becoming aware of a Breach. We shall make reasonable efforts to: (i) identify the cause of such Breach and take such steps as we deem necessary and reasonable to remediate the cause of such Breach to the extent the remediation is within our reasonable control, and (ii) provide you with information available to SMA Technologies regarding the Breach, including the nature of the incident, specific information disclosed (if known), and any relevant mitigation efforts or remediation measures, to allow you to meet your obligations under applicable Data Protection Laws due to a Breach. The obligations herein shall not apply to incidents that are caused by you or your Users.

7. **GOVERNMENT ACCESS REQUESTS.** In our role as a Processor, we shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense, and public security. If we receive a legally binding request to access Personal Data from a Regulator, we shall, unless otherwise legally prohibited, promptly notify you including a summary of the nature of the request. To the extent we are prohibited by law from providing such notification, we shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable us to communicate as much information as possible, as soon as possible. Further, we shall challenge the request if, after careful assessment, we conclude that there are reasonable grounds to consider that the request is unlawful. We shall pursue possibilities of appeal. When challenging a request, we shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. We shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. We agree to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. We shall promptly notify you if we become aware of any direct access by a Regulator to Personal Data and provide information available to us in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require SMA Technologies to pursue action or inaction that could result in civil or criminal penalty for SMA Technologies or its Affiliates such as contempt of court. We certify that SMA Technologies (i) has not purposefully created back doors or similar programming for the purpose of allowing access to the SMA Offerings and/or Personal Data by any Regulator; (ii) has not purposefully created or changed its business processes in a manner that facilitates access to the SMA Offerings and/or Personal Data by any Regulator; and (iii) at the Effective Date is not currently aware of any national law or government policy requiring SMA Technologies to create or maintain back doors, or to facilitate access to the SMA Offerings and/or Personal Data, to keep in its possession any encryption keys or to hand-over the encryption key to any third party.

8. **JURISDICTION SPECIFIC PROVISIONS.**

8.1 **CCPA**.

8.1.1 Personal Data. Subject to, and as except provided by, the CCPA, SMA Technologies will not: (A) sell or share Personal Data (as "sell" and "share" are interpreted under the CCPA); (B) retain, use, or disclose any Personal Data for SMA Technologies' commercial purpose; or (C) retain, use, or disclose the Personal Data outside of the direct business relationship between SMA Technologies and Customer. The parties further acknowledge and agree that our access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

8.1.2 Remediation Requirements. Customer shall have the right to take reasonable and appropriate steps to (i) verify that SMA Technologies uses the Personal Data that SMA Technologies receives from, or on behalf of, Customer in a manner consistent with this DPA so that Customer can meet its obligations under Data Protection Law. This right may encompass performing audits in accordance with this DPA; (ii) stopping and remediating SMA Technologies' unauthorized use of Personal Data; and (iii) taking any such other remediation efforts reasonably agreed upon by the parties. By way of example, and in accordance with the Agreement, Customer may require SMA Technologies to provide documentation that verifies that SMA Technologies no longer retains or uses Personal Data of Data Subjects who have made a valid request of Customer to delete their Personal Data.

8.1.3 Certification. SMA Technologies certifies that we understand and will comply with the obligations set forth in this DPA and the Agreement, including the restrictions on our Processing of Personal Data.

8.2 EUROPE. For purposes of this Section 8.2, the following capitalized terms have the meanings ascribed to them below:

"**Europe**" means all member nations of the European Economic Area (EEA), the United Kingdom (UK), and the Swiss Confederation (Switzerland).

"**EU Law**" means the GDPR, UK GDPR, and the Swiss Federal Act on Data Protection.

"**EU Standard Contractual Clauses**" means the standard contractual clauses approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as applicable, and available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.%20%20Module%202%20and%20Module%203 (referencing Module 2: Transfer Controller to Processor) and as may be amended or replaced by the European Commission from time-to-time.

"Restricted Transfer" means (a) where the GDPR applies, a transfer of Personal Data or Account Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (b) where the Swiss Federal Act on Data Protection applies, a transfer of Personal Data or Account Data from Switzerland to a country that is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commissioner; and (c) where the UK GDPR applies, a transfer of Personal Data or Account Data from the UK to a country that is not the subject of adequacy regulations under Section 17A of the United Kingdom Data Protection Act of 2018.

"**Standard Contractual Clauses**" means EU or UK government-approved contract mechanisms for the cross-border transfer of Personal Data from the EEA, Switzerland, or the UK (as applicable) to Third Countries.

"**Third Country(ies)**" means countries outside of the scope of the EU Laws, excluding countries approved as providing adequate protection for Personal Data by the applicable Regulators under EU Law.

"**UK Addendum**" shall mean the International Data Transfer Addendum issued by the Information Commissioner's Office and laid before Parliament on 2 February 2022 under Section 119(A) of the UK Data Protection Act 2018 as may be updated from time to time, currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

8.2.1 Penalties. Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any fines issued or levied under EU Law (*e.g.,* Article 83 of the GDPR) against the other party by a Regulator in connection with such other party's violation of EU Law.

8.2.2 Personal Data Transfers. To protect transfers of Personal Data out of Europe to Third Countries, the parties agree to enter into the Standard Contractual Clauses as described below:

8.2.2.1 Where a Restricted Transfer is made from the EEA, the EU Standard Contractual Clauses are incorporated into this DPA and apply to the transfer as follows: (i) with respect to Restricted Transfers from Customer to SMA Technologies, Module One applies where both Customer and SMA Technologies are Controllers, Module Two applies where Customer is a Controller and SMA Technologies is a Processor, and Module Three applies where both Customer and SMA Technologies are Processors; (ii) in Clause 7, the optional docking clause does not apply; (iii) in Clause 9(a) of Modules Two and Three, Option 2 applies, and the period for prior notice of subprocessor changes is set forth in Section 4 of this DPA; (iv) in Clause 11(a), the optional language does not apply; (v) in Clause 17, Option 1 applies with the governing law being that of Netherlands; (vi) in Clause 18(b), disputes will be resolved before the courts in Amsterdam (Netherlands); (vii) Appendix 1 of the SCCs is completed with the information in Appendix A to this DPA; (viii) Appendix 2 of the SCCs is completed with the information in Appendix B to this DPA; and (ix) Appendix C of the SCCs is completed with the list of Subprocessors referenced in Section 4.2.

8.2.2.2 Where a Restricted Transfer is made from Switzerland, the EU Standard Contractual Clauses are incorporated into this DPA and apply to the transfer as modified in Section 8.2.2.1, except that: (i) in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner if the Restricted Transfer is governed by the Swiss Federal Act on Data Protection; (ii) references to "Member State" in the EU Standard Contractual Clauses refer to Switzerland, and Data Subjects located in Switzerland may exercise and enforce their rights under the EU Standard Contractual Clauses in Switzerland; and (iii) references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the EU Standard Contractual Clauses refer to the Swiss Federal Act on Data Protection (as amended or replaced).

8.2.2.3 Where a Restricted Transfer is made from the UK, the UK Addendum is incorporated into this DPA and applies to the transfer. The UK Addendum is completed with the information in Section 8.2.2.1, Section 4.2, and Appendices A and B to this DPA; and both "Importer" and "Exporter" are selected in Table 4.

8.2.2.4 The following terms apply to the EU Standard Contractual Clauses: (i) Customer may exercise its audit rights under the EU Standard Contractual Clauses as set out in Section 5.2 above; (ii) SMA Technologies may appoint Subprocessors under the EU Standard Contractual Clauses as set

out in Section 4 above; (iii) with respect to Restricted Transfers made to SMA Technologies, we may neither participate in, nor permit any Subprocessor to participate in, any further Restricted Transfer unless the further Restricted Transfer is made in full compliance with Data Protection Laws and in accordance with applicable EU Standard Contractual Clauses or an alternative legally compliant transfer mechanism; and (iv) if any provision of this Section 8.2.2 is inconsistent with any terms in the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will prevail.

8.2.2.5 We may adopt a replacement data export mechanism (including any new version of or successor to the Standard Contractual Clauses or alternative mechanisms adopted pursuant to Data Protection Laws) ("**Alternative Transfer Mechanism**"), so long as the Alternative Transfer Mechanism complies with applicable Data Protection Laws and extends to the Third Countries to which Personal Data is transferred on behalf of the Customer. Customer agrees to execute documents and take other reasonably necessary actions to give legal effect to such Alternative Transfer Mechanism.

9. **LIMITATION OF LIABILITY.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between your Affiliates and SMA Technologies, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, our and our Affiliates' total liability for all claims from Customer and all of its Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Affiliate that is a contractual party to any such DPA.

10. **CONFLICT.** In the event of an actual conflict between the Agreement or this DPA, the terms and conditions in this DPA will control but only as to Processing of Personal Data.

11. **MODIFICATIONS.** We may make changes to this DPA where (i) the change is required to comply with applicable Data Protection Law; or (ii) the change is commercially reasonable, does not materially degrade or reduce the protective effect of the Security Measures, does not change the scope of our Processing of Personal Data, and does not have a material adverse impact on Customer's rights under this DPA.

12. **GOVERNING LAW AND JURISDICTION.** Unless prohibited by Data Protection Laws, this DPA is governed by the laws stipulated in the Agreement, and the parties to this DPA hereby submit to the choice of jurisdiction and venue stipulated in the Agreement, if any, with respect to any dispute arising under this DPA.

13. **GENERAL.** This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. The provisions of this DPA are severable. If any phrase, clause or provision or exhibit (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA or the remainder of the exhibit shall remain in full force and effect.

APPENDIX A

Details of Processing

(List of Parties, Description of Transfer, Competent Supervisory Authority)

A. LIST OF PARTIES

Data exporter:

Name: Contact details are identified in the Order Form.

Address: Contact details are identified in the Order Form.

Activities relevant to the data transferred under the clauses: The activities specified in Section 3 of the DPA.

Role (controller/processor): Controller

Data importer:

Name: The data importer is Unisoft International, Inc., dba SMA Technologies, a global provider of automation software and services.

Address: 46 N Main St, Kingwood, TX 77339United States.

Contact details: Legal; legal@smatechnologies.com.

Activities relevant to the data transferred under the clauses: The activities specified in Section 3 of the DPA.

Role (controller/processor): Processor

B. DESCRIPTION OF THE TRANSFER

Categories of Data subjects

The categories of data subjects whose personal data may be processed include: data exporter's customers, members, employees, consultants, contractors, agents, prospects, vendors, business partners and users authorized to use the Services; employees or contacts of third parties data exporter conducts business with.

Categories of personal data transferred

The personal data transferred may include the following categories of data: first and last name, professional title, contact information (email, phone number, physical address), username, identification data (IP address, device ID) and any other personal data provided through the services; depending on the data exporter's endpoint environment and naming conventions, data transferred may include personal data, such as that possibly found in a computer name, user name or file name. Specifically, Customers (Controller) may enable the SMA Offering to capture the following functional categories of data, with illustrative examples:

1. Account Data - account name, account username, customer pricing, and invoicing data associated with the user account.
2. Application Configuration Data – API keys, usernames, and passwords of account users.
3. Workflow History – Data indicating whether the data query mechanism (workflow) ran successfully.
4. Workflow Changelog - Data for auditing which user made changes to workflows, such as workflow name, version information, name of account user that made change, and time changes were made.
5. Workflow Data - Data sent to or pulled from applications during the run of a workflow, such as a piece of information from an end-user account for syncing or updating purposes.

Upon deployment of the SMA Offering, the Customer (Controller) configures workflows, determining and directing

data processing.

Sensitive data transferred (if appropriate)

The personal data transferred may include sensitive personal data, the extent of which is determined and controlled solely by the data exporter, and which may include: social security numbers, racial or ethnic origin; political opinions, religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; and data concerning sex life or sexual orientation.

Frequency of the transfer (e.g.) whether the data is transferred on a one-off or continuous basis

Personal data is transferred in accordance with the data importer's instructions as described in Section 2 of the DPA.

Nature of the Processing

The Personal Data will be processed for purposes of providing the services as described in the Agreement. The personal data transferred may be subject to the following basic processing activities: cloud-based storage, retrieval, erasure or destruction, disclosure by transmission, analysis, and any other processing necessary to provide and improve the services pursuant to the Agreement; to provide technical support; and otherwise in accordance with the data exporter's instructions or to comply with law.

Purpose(s) of the data transfer and further processing

To provide the Services under the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period, and how it is retained.

Retention. The duration of Processing will be as specified and in accordance with the published data retention policies under the Agreement and applicable product specifications. Data about the functioning of the software is stored for the Customer's use only as long as the Customer directs. Generally, when using the SMA Offering, workflow data is automatically purged from the system within one (1) hour after a workflow is done running ("Basic Retention"). However, if the data tracing feature is enabled by the Customer, data, including Personal Data will be retained for no more than six (6) calendar days after a workflow is enabled, before it is purged from the system. Data tracing may be "turned off" at any time and upon disablement, all data including Personal Data will be purged and the retention schedule will revert to Basic Retention.

How data is retained. When data, including Personal Data is being retained and is "at rest" in the SMA Technologies' system which is supported in part by our subprocessors. It is stored as protected and encrypted data.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

The personal data transferred may be disclosed to sub-processors of data importer solely as permitted by data importer to provide the services to data exporter under the Agreement, a current list of which is available at: **Appendix C.**

C. Competent Supervisory Authority

The data exporter's competent supervisory authority will be determined in accordance with GDPR.

APPENDIX B

Security Measures

A description of the technical and organisational security measures implemented by the data importer to ensure the security of Customer Data. Any capitalized term not otherwise defined herein shall have the meaning given in the Agreement.

1. Information Security Program

SMA maintains a written security program appropriate to the nature, size and complexity of SMA's business operations. The program complies with industry recognized information security frameworks, and includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data. The SMA information security official and security governance personnel continually review and update the security program policies, standards and operating procedures to ensure it retains relevancy and accuracy.

2. System and Network Security

a. Networks are logically segmented by Virtual Local Area Networks (VLANs) and firewalls monitor traffic to restrict access to authorized users, systems and services.

b. Firewall changes follow established processes and must be reviewed and approved.

c. Personnel access to SMA systems and networks is based on job responsibility. Access is promptly disabled when no longer required.

d. Network perimeter defense solutions including an Intrusion Detection System (IDS) and firewalls are in place to monitor, detect, and prevent malicious network activity. Security personnel monitor items detected and take action as appropriate.

3. Server and Endpoint Security

a. An endpoint management solution tool is used to deploy end-user devices and monitor software installed on endpoints.

b. Technology on SMA workstations monitors for virus and malware infections. Endpoint devices are scanned in real time. Virus definition updates are pushed to endpoint devices automatically.

c. Cloud servers are built using industry-standard security configuration management tools to set and enforce server security configurations based on industry-leading practices. Servers check in at frequent intervals for configuration updates.

d. Virtual servers are configured using a solution and adhere to the SMA server security configuration requirements. Access to the solution is restricted to authorized individuals. Creation, modification, and removal of virtual servers require appropriate authorizations.

4. User Access Controls

a. SMA personnel are required to identify and authenticate to the network with their unique user ID and password. Access to the SMA network is secured with multi-factor authentication (MFA). Password requirements are defined and enforced via a password tool.

b. Access to cloud systems is restricted to authorized individuals. Rigorous baseline password requirements for these systems are in place.

c. SMA enforces the rule of least privilege to restrict user access to only that needed to perform authorized functions. Successful and unsuccessful login attempts are logged.

d. SMA performs audits of administrator access to confidential and restricted systems, including the cloud production environment, on a regular basis. Any access by personnel who no longer require access based on job role is removed promptly.

e. Customers are required to enter a unique account user ID and a password to access the SMA system. The SMA system includes additional security configuration settings within the application, including an SSO option.

5. Physical Security

SMA does not directly use any physical data centers in its service of the Wripple product. However, SMA Technologies does use third-party Subprocessors such as Azure and Amazon Web Services as a cloud provider. These cloud providers host our applications in physical datacenters and they manage the infrastructure and physical security of these facilities.

6. Storage and Transmission Security

a. Industry-standard encryption technologies are used for data contained within, accessed by, or transmitted through the SMA system. Customer data is encrypted in transit and at rest.

b. Encryption keys are stored and transferred securely during the sign-in process using industry-standard encryption technology.

c. Customer file data transmitted to SMA is verified at multiple points after encryption at the source to provide destinations the ability to detect tampering or corruption.

7. Monitoring and Logging

a. SMA monitors server, storage, and network devices on a real-time basis for operational performance, capacity, and availability metrics. System dashboards are configured to alert when predefined thresholds are exceeded.

b. Incident management and escalation procedures exist to address system issues, problems and security-related events, in a timely manner. Incidents are logged, prioritized, and resolved based on established criteria and severity levels.

c. For SMA laptops and select applications, SMA utilizes a security information event monitoring system to pull real-time security log information from servers, firewalls, routers, intrusion detection system devices, end users, and administrator activity. The SIEM is configured for alerts and monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events and are reviewed by the security team.

8. Software and Application Security

a. SMA has established a Software Development Life Cycle (SDLC) process to govern the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components.

b. SMA utilizes a code versioning control system to maintain the integrity and security of the application source code.

c. Product releases undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment.

d. Regular internal and external vulnerability scans are conducted using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated and remediated to address the associated risk(s).

e. External application penetration tests are conducted by an independent third party at least annually. Critical findings from these tests are evaluated, documented and remediated.

9. Instructions to Personnel

a. All personnel sign a confidentiality agreement as part of their employment contract.

b. All personnel are required to complete security training upon hire and on a periodic basis. Security training includes, at a minimum:

   i. Security education and communications.

ii. General and role-specific security training.

iii. Ongoing phishing tests.

iv. Instructions on how to report security incidents.

v. Responsibilities regarding data privacy and security.

10. Ensuring Availability

a. To meet customer availability commitments, capacity demand is reviewed and evaluated at appropriate intervals for corrective actions, if needed.

b. Regular maintenance windows exist for both system maintenance and release maintenance (new features, enhancements, and fixes to SMA products).

c. SMA maintains a business continuity plan and a disaster recovery plan to manage significant disruptions to SMA operations and infrastructure. The plans are updated as needed, but at least annually, and approved by the lead of the information security function.

11. Certifications and Assessments

SMA conducts third party audits to attest to various frameworks including SOC 2 Type 1, and penetration testing.

12. Data Storage and Erasure

For customer data collected by SMA, customer agreement files are retained for the duration that SMA provides the Services and a period after to permit SMA to comply with business obligations such as filing taxes. Data about the functioning and auditing of the software is stored for the Customer's use the shorter of the period while SMA provides the services, or as long as the Customer directs. Wripple workflow data is automatically purged from processor (SMA) system within one hour after the applicable workflow is done running. Customer data is permanently deleted in accordance with industry recognized standards for data destruction.

13. Sub-processor Compliance

SMA has an established process to assess and manage third party sub-processors. All sub-processors are contractually obligated to comply with the security requirements established in this Appendix, or in any event, requirements that are substantially similar or equivalent. The security team performs a security review of sub-processors during an onboarding process and at least annually thereafter.

14. **Incident Response**

We maintain industry-recognized security incident management policies and procedures and shall notify you without undue delay after becoming aware of a Breach. We shall make reasonable efforts to: (i) identify the cause of such Breach and take such steps as we deem necessary and reasonable to remediate the cause of such Breach to the extent the remediation is within our reasonable control, and (ii) provide you with information available to SMA Technologies regarding the Breach, including the nature of the incident, specific information disclosed (if known), and any relevant mitigation efforts or remediation measures, to allow you to meet your obligations under applicable Data Protection Laws due to a Breach. The obligations herein shall not apply to incidents that are caused by you or your Users.

Appendix C

Subprocessors

The Subprocessors are:

- Gainsight, Inc.,
- Azure, a cloud service provider, and
- Amazon Web Services (AWS),

which may be amended or changed from time to time.

Appendix D

UK Addendum

International Data Transfer Addendum to the EU SCCs

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Effective Date as set out in the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out at the top of the Appendix 1	As set out at the top of the Appendix 1

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	Means the EU SCCs as defined in the Addendum

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	As set out at the top of the Addendum and Appendix A, Annex 1
Annex 1B: Description of Transfer:	Annex 1 of the Appendix A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	Annex 2 of the Appendix B
Annex III: List of Sub processors (Modules 2 and 3 only):	Appendix C

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☒ Importer

Addendum changes	☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0, in force 21 March 2022, issued by the ICO, as it is revised under Section 18 of those Mandatory Clauses, are hereby incorporated.