DATA PROCESSING AGREEMENT

This Data Processing Agreement, (the "***DPA***") is made by and between **SaaS Consulting Group, LLC**, a Texas limited liability company, having a principal place of business at 504 Congress Avenue, Third Floor, Austin, TX 78701 USA ("**Data Controller**") and the Customer, as defined in the Master Services Agreement and/or Subscription Services Agreement ("**Data Processor**"), (each a "**Party**", and collectively the "**Parties**"). This DPA is effective and shall remain in force for the term of the Master Services Agreement and/or Subscription Services Agreement.

1. **Purpose of the DPA.** The Parties have executed an agreement for the provision, performance and/or delivery of services by the Data Processor to the Data Controller whereby the Data Processor may process Personal Data, as defined in Section 2 (c) of this DPA, obtained by and on behalf of the Data Controller, which may be a Master Services Agreement and/or a Subscription Services Agreement (individually or collectively, the "**Agreement"**).

2. **Definitions.** The following defined terms are used in this DPA, together with other terms defined herein.

   a) "**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under this DPA.

   b) "**Data Subject**" means the individual to whom Personal Data relates.

   c) "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

   d) "**Processing (or Process)**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction.

3. **Processing of Data.**

   a) Data Controller's Processing of Personal Data. Data Controller will Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Data Controller's instructions for the Processing of Personal Data will comply with Data Protection Laws and Regulations. Data Controller is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Data Controller acquired Personal Data.

   b) Data Processor's Processing of Personal Data. Data Processor will only Process Personal Data on behalf of and in accordance with Data Controller's instructions and in relation to the Agreement and its purpose (the "Purpose"), and will treat Personal Data as Confidential Information. By entering into this DPA, Data Controller instructs Data Processor to Process Personal Data in accordance with the Purpose. Data Controller may issue additional instructions to Data Processor, and Data Processor shall promptly comply with all such additional instructions, as long as such instructions (i) comply with applicable Data Protection Laws and Regulations, (ii) are issued by Data Controller to Data Processor in writing and with sufficient advance notice for Data Processor to review, consider and act on such instructions, do not provide Data Processor with additional sensitive or special Personal Data that imposes additional data security or data protection obligations on Data Processor beyond those which are already contemplated in the Agreement (iii) and (iv) Data Processor has the means and authority to so act. To the extent that Data Processor expects to incur additional charges or fees not contemplated or covered by the Agreement and with respect to any additional instructions, the Parties shall, without prejudice, negotiate in good faith as to which Party or Parties bear the cost of the additional instructions.

   c) Subprocessing of Personal Data. Data Controller permits Data Processor to use subprocessors to Process Personal Data; provided, that Data Processor enters into an agreement with each subprocessor that contains terms no less restrictive than this DPA and that complies with the Data Protection Laws and Regulations. Data Processor will provide Data Controller with sixty (60) calendar days advance notice prior to using a new subprocessor to Process Personal Data for the Purpose. Data Controller may terminate this DPA if the new

subprocessor is unacceptable to Data Controller.

4. **Rights of Data Subjects.**

a) Correction, Blocking and Deletion. To the extent Data Controller does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, Data Processor will comply with any commercially reasonable request by Data Controller to facilitate such actions to the extent Data Processor is legally permitted to do so. Data Controller is responsible for any costs arising from Data Processor's assistance.

b) Data Subject Requests. Data Processor will, to the extent legally permitted, promptly notify Data Controller if it receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. Data Processor will not respond to any such Data Subject request without Data Controller's prior written consent except to confirm that the request relates to Data Controller. Data Processor will provide Data Controller with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Data Controller does not have access to such Personal Data. Data Controller is responsible for any costs arising from Data Processor's assistance.

5. **Data Processor Personnel.**

a) Confidentiality. Data Processor will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Data Processor will ensure that such confidentiality obligations survive the termination of the personnel engagement.

b) Reliability. Data Processor will take commercially reasonable steps to ensure the reliability of any Data Processor personnel engaged in the Processing of Personal Data.

c) Limitation of Access. Data Processor will ensure that access to Personal Data is limited to those personnel performing services in accordance with the Agreement.

d) Data Protection Officer. Data Processor has appointed a corporate officer to oversee and otherwise manage its data protection responsibilities and obligations. The appointed person may be reached at legal@saascg.com.

6. **Security.** Data Processor maintains adequate administrative, physical, and technical safeguards for protection of the security (including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage), confidentiality, and integrity of Personal Data.

7. **Security Breach Management and Notification.** Data Processor maintains security incident management policies and procedures, and will, to the extent permitted by law, promptly notify Data Controller of any actual or reasonably suspected unauthorized disclosure of Personal Data, of which Data Processor becomes aware (a "**Security Breach**"). To the extent such Security Breach is caused by a violation of the requirements of this DPA, Data Processor will make reasonable efforts to identify and remediate the cause of such Security Breach.

8. **EU-US Transfers.** For the purposes of Article 26(2) of Directive 95/46/EC as it may relate to the Processing of Personal Data that is transferred from the European Economic Area to the United States, Data Controller and Data Processor have agreed on the Standard Contractual Clauses described in Schedule 1 in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data described in Schedule 1.

9. **Audits.**

a) Data Processor. Data Processor allows for, cooperates with, and contributes to audits, including inspections, conducted by Data Controller or an external auditor engaged by Data Controller. Audits may be conducted: (i) from time to time on reasonable notice, but no more frequently than once per calendar year; (ii) during normal business hours and so as not to unreasonably interfere with Data Processor's performance of the services or

unreasonably interfere with Data Processor's business; and (iii) during the term of this DPA. The notice requirement in clause 9(a)(i) and the restrictions stated in 9(a)(ii) shall not apply to the extent the audit is initiated by a regulator. Data Processor shall provide to Data Controller and its auditors and regulators reasonable assistance as they require for the purpose of performing an audit, including access to the following: the place, premises and facilities from which the services will be performed; the systems (including software, networks, firewalls and servers) used to perform the service; and data, records, manuals and other information relating to the services. Each Party shall bear its own costs in relation to the audit. If an audit results in Data Processor being notified that it, or its Processing of Personal Data, is not in compliance with Data Protection Laws and Regulations, the Parties shall discuss such finding and, with respect to any such non-compliance, Data Processor shall promptly take all corrective actions necessary to achieve compliance to the satisfaction of Data Controller. Where any audit report prepared by Data Processor's internal or external auditors contains information relating to the Personal Data, Data Processor shall promptly disclose such information to Data Controller.

b) Subprocessor. Data Processor will facilitate, cooperate, and assist with Data Controller's audit of any subprocessor. If an audit results in Data Processor being notified that the subprocessor, or its Processing of Personal Data, is not in compliance with Data Protection Laws and Regulations, the Parties shall discuss such finding and, with respect to any such non-compliance, Data Processor shall promptly take all corrective actions necessary to achieve compliance to the satisfaction of Data Controller including, but not limited to, replacing the subprocessor with a new subprocessor acceptable to Data Controller. If Data Processor breaches its obligations under this Section, Data Controller may terminate this DPA.

10. Updates. This DPA may be amended from time to time as necessary by the Data Processor. Data Processor shall maintain version documentation for each DPA, and shall provide at least thirty (30) days written notice to Customers of any updates to the DPA.

11. **Miscellaneous**. This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior understandings regarding such subject matter, whether written or oral. To the extent a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. This DPA will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns. Data Controller may assign this DPA to an affiliate or in connection with a merger of Data Controller or the sale of substantially all of Data Controller's assets. If this DPA is translated into languages other than English, the English version will control. If for any reason, a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect. No amendment or modification of this DPA will be binding unless in writing and signed by Data Controller. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA shall survive such termination.

12. **Authority of Signatories**. Each person signing the Agreement represents and warrants that he or she is duly authorized and has legal capacity to execute this DPA.

Schedule 1 – Standard Contractual Clauses

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations

of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or

in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

The Data Controller.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

The Data Processor in performing services described in Section 1 of the DPA.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

The Data Controller's employees, prospects, customers, vendors, agents, contractors, representatives, end users, partners, and similar.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Personal contact information, such as names, email addresses, physical home addresses, home and mobile telephone numbers, fax numbers, date of birth, marital status, employment details including employer name, job title and function, employment history, salary and other benefits, job performance details, education/qualification, identification numbers, business contact details, financial details, goods and services provided history, IP addresses, online behavior, unique IDs collected from mobile devices, network carriers or data providers, online behavior and interest data, and other related general identification and categorization information that may have been captured by Data Con

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

The performance and/or delivery of the Services pursuant to the Agreement (Master Services Agreement and/or Subscription Services Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

SaaS Consulting Group, LLC (SCG) shall, at all times, deploy and maintain appropriate control measures designed to prevent or detect data privacy or information security breaches or violations by a SCG employee, contractor, or agent performing or delivering the Services. Specifically, SCG agrees that: (a) it will only access portions of the Customer's IT Environment for which Customer has explicitly granted or provisioned to SCG, (b) it will only share such access with its employees, contractors or agents on a need-to-know basis and only as it relates to the performance or delivery of the Services, and (c) it will not act or engage in practices that could in any way subvert or compromise the security, integrity, or operating effectiveness of Customer's IT Environment, or the accuracy and authentication of transactions processed by and through Customer's Application.

In addition, Services shall only be performed by SCG employees (1) for whom SCG has conducted a satisfactory criminal background check screening, (2) who have acknowledged and signed confidential agreements with SCG as part of their employment, and (3) who have acknowledged and signed SCG's BYOD and Acceptable Use Policy, which includes (a) the requirement for employee devices to have hard drive encryption (at rest) enabled at all times, (b) the requirement for employee and subcontractor devices to have installed an actively managed endpoint threat monitoring, detection and protection application deployed and managed by SCG, (c) password standards, and (d) the employee's responsibilities for protecting Customer data.