DATA PROTECTION AGREEMENT (Processor)

This Data Protection Agreement, including any Annexes attached hereto ("DPA"), is made and entered into effective as of <Month Day, 2019> ("Effective Date") by and between ASG Technologies Group, Inc., with its principal place of business at 708 Goodlette Road North <if applicable: a United States corporation, through its <Local Country, Subsidiary or Branch> located at <Street Address> <City> <State> <Country> ("ASG" or the "Data Processor"), and <Client Legal Entity Name>, a <Country> <Corporation> with its principal place of business at <Street Address>, <City>, <State> <Zip> ("Client" or the "Data Controller").

WHEREAS, Client and ASG have executed and entered into a …… Software License Agreement together with appended Product Schedule(s) *(please specify further)* dated _____ (the "Agreement") **OR** *purchase order dated* _____ *(please specify further)* for the licensing and maintenance and support of licensed ASG software *(the "Agreement")* and it cannot be excluded that such maintenance and support services may involve processing by ASG of Personal Data belonging to Client as the Data Controller, and such contractual relationship and processing being subject to Applicable Data Protection Laws;

WHEREAS, ASG will carry out a processing on behalf of the Data Controller, in order to be able to provide the contracted services in accordance with Applicable Data Protection Laws; AND

WHEREAS, the Data Controller wishes to ensure that ASG offers sufficient guarantees to apply appropriate technical and organizational measures, so that the processing complies with the requirements of Applicable Data Protection Laws and guarantees the protection of the rights of the natural persons as data subjects.

NOW AND THEREFORE, it is understood and agreed as follows:

1. DEFINITIONS

1.1. 'Applicable Data Protection Law' means any applicable regulation or legislation within the jurisdiction agreed in the Agreement **OR** *[insert here the jurisdiction applicable to ASG's principal place of business / the < place of business of the Local Branch/Subsidiary>*, including any regulatory guidance by a Supervisory Authority, which protects the fundamental rights and freedoms of individuals and their right to privacy with respect to the Processing of Personal Data under the Agreement. the Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons in the processing of personal data ("GDPR" or the "Regulation") representing the minimum standard regardless of whether the Personal Data is subject to GDPR or not.

1.2. 'Data Controller' means the Client which makes available to ASG the Personal Data and determines the purposes and means of the Processing.

1.3. 'Data Processor' means ASG which agrees to be provided by or receive from the Data Controller the Personal Data intended for Processing on Data Controller's behalf after the provision or transfer in accordance with Data Controller's instructions and the terms of this DPA. ASG may transfer the Personal Data to a third country only in accordance with Section 8. Cross-border Processing.

1.4. 'Data Subject' means a living natural person which can be uniquely identified and which shall enjoy the protection of its Personal Data under Applicable Data Protection Law.

1.5. 'Personal Data' means any information relating to a Data Subject which directly or indirectly, on its own or in combination with another identifier, clearly identifies the Data Subject and therefore must be afforded protection under Applicable Data Protection Law.

1.6. 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed or any incident involving Personal Data beyond the scope of regular Processing foreseen by the Agreement and in each case Data Controller is required under Applicable Data Protection Law to provide notice to the Supervisory Authority or Data Subjects.

1.7. 'Processing' means any operation or set of operations which is performed on Data Controller's Personal Data, whether or not by automated 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, erasure or destruction.

1.8. 'Standard Contractual Clauses" (also referred to as "EU Model Clauses") means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of this DPA are attached hereto as Appendix 3.

1.9. 'Supervisory Authority' shall mean any official authority or body authorized under Applicable Data Protection Law to monitor, audit, inspect, ensure the safeguarding and enforcement of the rights and freedoms of Data Subjects under said law.

1.10. 'Sub-processor' means any processor engaged by ASG or by any other sub-processor of ASG who agrees to receive from ASG or from any other sub-processor of ASG Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Controller after the transfer in accordance with its instructions, the terms of the Agreement, this DPA and the terms of the written subcontract.

1.11. 'Technical and Organizational Measures' means those measures aimed at protecting the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. ASG shall fill out Annex 1 – Technical and Organizational Measures which becomes an integral part of this Agreement.

2. PROCESSING PURPOSE

2.1. The purpose of the Processing is to enable ASG to provide the contracted services under the Agreement and establish the terms and conditions under which access to the Personal Data by ASG must be carried out.

3. IDENTIFICATION OF THE INFORMATION PROVIDED

For the execution of the agreed services, ASG may have access to information detailed below:

3.1. Categories of Data Subjects: _____

_____

3.2. Categories of data: _____

_____

3.3. Special Categories of data: _____

_____

4. OBLIGATIONS OF THE DATA PROCESSOR

4.1. Technical and Organizational Measures. ASG confirms that it has implemented the Technical and Organizational Measures specified in Annex 1 before access and/or receipt and processing the Personal Data in such manner as to satisfy the particular requirements of Applicable Data Protection Law. Client shall implement such measures as required under GDPR in order to ensure permanently compliance and the confidentiality, integrity, availability and resilience of its systems and services in connection with the services under the Agreement.

4.2. Duty of Confidentiality. ASG shall maintain the duty of confidentiality regarding the Personal Data to which ASG has or has had access, even after completion of the Processing purpose or which remains in ASG's possession after termination of this Agreement. ASG guarantees that any persons authorized to Process the Data Controller's Personal Data shall be obliged in writing to the same level of confidentiality and to comply with the same security measures of which they have been be notified accordingly.

4.3. Processing. ASG shall use the Personal Data intended for processing, or as received or made available by the Data Controller, and only for the purpose of the contracted services under the Agreement. In no case may Client use the Personal Data for its own purpose. ASG shall process the Personal Data only on behalf of the Data Controller and in compliance with its instructions and the Agreement. If ASG cannot provide such compliance for whatever reasons, it agrees to inform the Data Controller promptly of its inability to comply, in which case the Data Controller is entitled to block access to or suspend the transfer of the Personal Data immediately and/or terminate the contract.

4.4. Applicable Data Protection Law. ASG certifies that it has no reason to believe that the Applicable Data Protection Law prevents it from fulfilling the instructions received from the Data Controller and the obligations under the Agreement. ASG agrees, that in the event of a change in the Applicable Data Protection Law which is likely to have a substantial adverse effect on the guarantees and obligations provided by this DPA, it will promptly notify the Data Controller of any such change as soon as it becomes aware. In this case the Data Controller is entitled to block access to or suspend the transfer of the Personal Data and/or terminate the contract.

4.5. Notification. ASG will promptly notify the controller about:

4.5.1. 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;

4.5.2. any accidental or unauthorized access; and

4.5.3. any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorized to do so.

4.6. Enquiries. ASG shall deal promptly and properly with all inquiries from the Data Controller relating to its processing of the Personal Data subject to the processing and to abide by the advice of the Supervisory Authority with regard to the processing of such data.

4.7. Reserved.

4.8. Audit and Security Assessments. ASG shall maintain complete and accurate records relation to its data protection practices in relation to services provided under the Agreement, the security of Data Controller's data, including any backup, disaster recovery, or other policies, practices,

or procedures; the security of its core functional processes; and any other information relevant to its compliance with this DPA. At the reasonable prior written request of the Data Controller, but not more than once annually, or Data Controller's reasonable suspicion of a security breach or ASG's violation of this DPA, ASG shall submit its data-processing facilities for audit of the processing activities covered by this DPA. The audit shall be carried out by the Data Controller or a professional auditor, instructed by the Data Controller. Such auditor shall possess the required professional qualifications and be bound by a duty of confidentiality. Any audit shall take place during normal business hours and not unnecessarily disrupt ASG's daily operations. The audit may consist instead of a security questionnaire to help answer sufficiently Client's questions regarding ASG's services under the Agreement. Data Controller or its authorized auditors shall only have access to table of contents or, where permitted, appropriate summaries or excerpts of ASG records as relating to its data protection practices. Each party shall bear its own costs and expenses in respect of such audit or security questionnaires.

4.9. Corrective Measures. If any audit or security questionnaire or in ASG's data protection practices uncovers deficiencies or identifies suggested changes in ASG's performance of services under the Agreement, ASG shall immediately within a reasonable time take the necessary corrective measures to satisfy the findings and recommendations of Client's professional auditors.

4.10. Sub-contractors. ASG shall only be permitted to use sub-processor(s) if ASG has agreed adequate data protection and security measures processing services in accordance with section 7.

4.11. Data Protection Officer. ASG confirms to have appointed a data protection officer, representative or person of similar role and function who will monitor and ensure Client's compliance with Applicable Data Protection Laws. The Data Protection Officer's contact details are as follows: _____.

5. OBLIGATIONS OF THE DATA CONTROLLER

The Data Controller agrees and warrants that:

5.1. It will inform ASG promptly and adequately if it discovers errors or irregularities in the Processing in respect of Applicable Data Protection Law.

5.2. it has instructed, and throughout the duration of the Processing, will instruct ASG to access and process the Personal Data only on the Data Controller's behalf and in accordance with the Applicable Data Protection Law, the Agreement and this DPA.

5.3. 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 the GDPR, in which case ASG and Data Controller shall execute Standard Contractual Clauses in accordance with Section 8 below.

5.4. to forward any notification received from the processor or any sub-processor to the Supervisory Authority if the Data Controller decides to continue the Processing, transfer or to lift the suspension.

6. SECURITY BREACH

The Parties agree and warrant:

6.1. In the event of a suspected Security Breach, ASG will:

6.1.1. Take action immediately, at ASG's own expense, to investigate the suspected Security Breach and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach.

6.1.2. notify the Data Controller immediately to privacy@asg.com within 72 hours if there are causes to believe that a Security Breach has in fact occurred and provide the Data Controller with a detailed description of the Security Breach including:

6.1.2.1. the likely impact of the Security Breach;

6.1.2.2. the categories and approximate number of data subjects affected and their country of residence and the categories and approximate number of records affected;

6.1.2.3. the risk posed by the Security Breach to individuals;

6.1.2.4. the measures taken or proposed to be taken by ASG to address the Security Breach and to mitigate its adverse effects;

6.1.2.5. provide timely updates to this information and any other information Data Controller may reasonably request relating to the Security Breach; and

6.1.2.6. except to the extent required by law, not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without Data Controller's prior written approval.

6.1.2.7. ASG will indemnify and hold the Data Controller harmless against all losses, claims, costs, damages or proceedings suffered or incurred by the Data Controller arising out of or in connection with ASG breach of this Section 6.1.

6.1.3. ASG will support the Data Controller in carrying out the impact assessments regarding data protection, where appropriate.

6.1.4. ASG will support the Data Controller in carrying out the prior consultations with the Supervisory Authorities.

7. SUB-PROCESSING

7.1. The Data Processor shall not subcontract any of its processing operations performed on behalf of the Data Controller under this Agreement without the prior written consent of the Data Controller. Where ASG subcontracts its obligations under the DPA, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the processor under this DPA. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations under such agreement.

7.2. ASG has instructed the following sub-processors with all or parts of the services under the Agreement:

Company name and registered address	**Description of (partial) services**

7.3. The provisions relating to data protection aspects for the sub-processing contract shall be governed by applicable jurisdiction.

8. CROSS-BORDER PROCESSING

8.1. Conditions for International Processing. Client shall be entitled to process Personal Data only in accordance with this DPA outside the country in which the Data Controller is located as permitted under Applicable Data Protection Law.

8.2. Standard Contractual Clauses. Where (i) Personal Data of the Data Controller based in a member country of the EEA is processed in a country outside the EEA and any country acknowledged by the European Union as a safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of the Data Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Data Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

8.2.1. ASG and Data Controller shall execute the Standard Contractual Clauses;

8.2.2. ASG's sub-processors shall enter into the Standard Contractual Clauses with Data Controller as follows: either (i) the relevant sub-processor joins the Standard Contractual Clauses entered into by ASG and the sub-processor as an independent owner of rights and obligations ("Accession Model") or, (ii) the sub-processor (represented by ASG) enters into the Standard Contractual Clauses with the Data Controller ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when Data Controller has expressly confirmed that a sub-processor is eligible for it through the sub-processor list provided under Section 7.2 or upon prior written notice to ASG.

8.3. Relation of the Standard Contractual Clauses to the DPA. Nothing in the DPA shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and sub-processor rules in sections 4 and 7, such specifications also apply in relation to the Standard Contractual Clauses.

8.4. Governing Law Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Data Controller is incorporated.

9. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA-PROCESSING SERVICES

9.1. The parties agree that on the termination of the Agreement, the Data Processor shall, at the choice of the Data Controller, return all the Personal Data and the copies thereof to the Data Controller or shall destroy all the Personal Data and certify that it has done so, unless legislation imposed upon ASG prevents it from returning or destroying all or part of the Personal Data. In that case, the Data Processor warrants that it will guarantee the confidentiality of the Personal Data and will not actively process it anymore.

10. LIABILITY

10.1. Without prejudice to the provisions of Articles 82, 83 and 84 of the GDPR, if ASG infringes this DPA in determining the purposes and means thereof, it shall be considered as a data controller. Likewise, ASG will be responsible for any damage to third parties committed by it, due to the non-fulfillment of its obligations as a processor, and which will result in a possible claim against the Data Controller filed by an interested third party. In this regard, ASG shall indemnify the Data Controller for any penalties, charges, legal fees and damages under such claim.

10.2. In any case, the Data Controller shall notify ASG of any claims and provide reasonably requested assistance in the defense of the same.

11. MEDIATION AND JURISDICTION

11.1. The Data Processor agrees that if a data subject invokes against it third-party beneficiary rights and/or claims for compensation of damages under this DPA, the Data Processor will accept the decision of the data subject:

11.1.1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority.

11.1.2. to refer the dispute to the courts in the Member State in which the controller is established.

11.2. 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.

12. Governing law

12.1. This DPA shall be governed by and construed and enforced in accordance with the laws of [*please insert as applicable]* <the State of Florida> **OR** <the place of business of the ASG's Branch / Subsidiary>. Any action or proceeding arising from this DPA shall be brought in the courts of [*please insert as applicable*> and the parties hereby consent to be subject to this jurisdiction.

13. Variation of the contract

13.1. The parties undertake not to vary or modify this Agreement unless in writing and signed by authorized legal representatives.

THIS DPA IS HEREBY ACCEPTED AND AGREED TO BY BOTH CLIENT AND ASG.

Company:	ASG Technologies Group, Inc.	Company:	
Address:	708 Goodlette Road North		
	Naples, Florida 34102		
By:		By:	
Name:		Name:	
Title:		Title:	
Date:		Date:	

ANNEX 1 - TECHNICAL AND ORGANIZATIONAL MEASURES (TOMS)

1. PSEUDONYMIZATION AND ENCRYPTION OF PERSONAL DATA (Art. 32 para. 1 (a) of the GDPR)

- **Pseudonymization**

  Processing personal data in a manner such that personal data can no longer be attributed to any specific data subject without consulting additional information, provided that this additional information is kept in a separate location and is subject technical and organizational measures.

  Description of measures taken:

  _____

  _____

- **Encryption**

  Use of procedures and algorithms that convert personal data into non-readable form by using digital or electronic codes or keys. Symmetric and asymmetric encryption technologies may be used:

  Description of measures taken: Please provide sufficient details

  _____

  _____

2. MEASURES TO ENSURE CONFIDENTIALITY (Art. 32 para. 1 (b) of the GDPR)

- **Physical access control**

  Technical and organizational measures for physical access control, including, without limitation, identification of authorized persons:

  Description of measures taken: Please provide sufficient detail

  _____

  _____

- **System access control**

  Technical measures (keyword/password protection) and organizational measures (user master data set) for user identification and authentication:

  Description of measures taken: Please provide sufficient detail

  _____

- **Data access control**

  Access authorization and data access rights granted on need-to-know basis, as well as monitoring and tracking access:

  Description of measures taken: Please provide sufficient detail

- **Separation control**

  Measures to ensure separate processing (storage, modification, erasure, transmission) of data serving different purposes:

  Description of measures taken: Please provide sufficient detail

3. MEASURES TO ENSURE INTEGRITY (Art. 32 para. 1 (b) of the GDPR

- **Transfer control**

  Measures for migration, transfer, transmission, or storage of data to or on data carriers (manually or electronically), and measures for subsequent review:

  Description of measures taken: Please provide sufficient detail

- **Input control**

  Measures for subsequent review whether and by whom data were input, modified, or removed (erased):

  Description of measures taken: Please provide sufficient detail

4. AVAILABILITY AND RESILIENCE OF SYSTEMS AND SERVICEs (Art. 32 (b) of the GDPR)

- **Availability control**

  Measures for (physical/logical) data backup:

  Description of measures taken: Please provide sufficient detail

  _____

- **Availability of IT systems used**

  Description of measures taken: Please provide sufficient detail

  _____

5. MEASURES TO RESTORE AVAILABILITY AND ACCESS TO PERSONAL DATA IN THE EVENT OF A TECHNICAL INCIDENT (Art. 32 (c) of the GDPR)

- **Recovery/backup systems**

  Description of measures taken: Please provide sufficient detail

  _____

  _____

6. PROCEDURES FOR THE REGULAR REVIEW, ASSESSMENT, AND EVALUATION OF TECHNICAL AND ORGANIZATIONAL MEASURES (Certifications, recovery plans, business continuity plan, penetration testing etc… (Art. 32 para. 1 (d) of the GDPR. Art. 25 para. 1 of the GDPR)

Description of measures taken:

_____

_____