DATA PROCESSING ADDENDUM

Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU - Standard Contractual Clauses (Processors)

This Data Processing Addendum ("DPA") forms part of the End User License Agreement (or other such titled written or electronic agreement addressing the same subject matter) between RSSBUS and Customer for the purchase of software and technical support services from RSSBUS (collectively identified as "Services"), wherein such End User License Agreement is hereinafter defined as the "Agreement," and whereby this DPA reflects the parties' agreement with regard to the Processing of Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent RSSBUS processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, RSSBUS may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Attachment 1 (including Appendices 1 to 3).

2. This DPA has been pre-signed on behalf of RSSBUS LLC. The EU Standard Contractual Clauses in Attachment 1 (including Appendices 1 to 3) have been pre-signed by RSSBUS LLC. as the data importer.

3. To complete this DPA, Customer must:
    a. Complete the information in the signature box and sign on Page 5
    b. Complete the information as the data exporter on Page 6
    c. Complete the information in the signature box and sign on Pages 11, 12, 14, 15 and 16

4. Send the completed and signed DPA to RSSBUS by email to gdpr@rssbus.com.

Upon receipt of the validly completed DPA by RSSBUS at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to and forms part of the Agreement. In such case, the RSSBUS entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with RSSBUS or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the RSSBUS entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is not a party to an Order Form nor an End User License Agreement directly with RSSBUS but is instead a customer indirectly via an authorized reseller of Services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and RSSBUS but has not signed its own Order Form with RSSBUS and is not a "Customer" as defined under the Agreement.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer Data**" means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Services.

"**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 the Agreement.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"**Processing**" (including its root word, "**Process**") shall have the meaning given in Data Protection Laws and Regulations.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**RSSBUS**" means the RSSBUS entity which is a party to this DPA, as specified in the Section "How This DPA Applies" above, being RSSBUS LLC., a limited liability corporation incorporated in North Carolina and its primary address as 101 Europa Drive, Suite 110, Chapel Hill, NC, USA, or an Affiliate of RSSBUS, as applicable.

"**RSSBUS Group**" means RSSBUS and its Affiliates engaged in the Processing of Personal Data.

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and RSSBUS and included herein, pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Sub-processor**" means any Processor engaged by RSSBUS or a member of the RSSBUS Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, RSSBUS is the Processor and that RSSBUS or members of the RSSBUS Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Services, comply with Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data must comply with Data Protection Laws and Regulations. In addition, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services.

2.3. RSSBUS' Processing of Personal Data. RSSBUS will process and use Customer Data and Personal Data on Customer's behalf and only in accordance with Customer's instructions (including via email) and to the extent required by law, including but not limited to the GDPR requirements directly applicable to RSSBUS' provision of the Services. Customer hereby acknowledges that by virtue of using the Services it gives RSSBUS instructions to process and use Customer Data and Personal Data in order to provide the Services in accordance with the Agreement. Customer takes full responsibility to keep the amount of Customer Data and Personal Data provided to RSSBUS to the minimum necessary for the performance of the Services.

2.4. Scope of Processing. The subject matter of Processing of Personal Data by RSSBUS is the provision of the Services pursuant to the Agreement. The nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in Attachment 1, Appendix 1 to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. Data Subject Requests. RSSBUS shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Laws and Regulations, including its rights of access, correction, objection, erasure ("right to be forgotten"), data portability, or to not be subject to an automated individual decision making (each, a **"Data Subject Request"**); and (ii) any other correspondence, inquiry or complaint received from a Data Subject, Supervisory Authority, or other third party in connection with the Processing of the Data to the extent RSSBUS is legally permitted to do so and that the response to such Data Subject Request is required under applicable Data Protection Laws and Regulations. Customer shall be responsible for any costs arising from RSSBUS' provision of such assistance, including any fees associated with providing additional functionality. In the event that any such request, correspondence, inquiry or complaint is made directly to RSSBUS, RSSBUS shall promptly inform Customer providing full details of the same.

4. RSSBUS PERSONNEL

4.1. Confidentiality. RSSBUS shall 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. RSSBUS shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. RSSBUS shall take commercially reasonable steps to ensure the reliability of any RSSBUS personnel engaged in the Processing of Personal Data.

4.3. Limitation of Access. RSSBUS shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4. Data Protection Officer. RSSBUS is not required to officially appoint a data protection officer to the extent this is required by Data Protection Laws and Regulations. However, upon request, Customer may contact gdpr@RSSBUS.com with any questions or requests under this DPA.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that (i) RSSBUS is entitled to retain its Affiliates as Sub-processors, and (ii) RSSBUS or any such Affiliate may engage any third parties from time to time to process Customer Data in connection with making the Software and/or the provision of Support. RSSBUS will only disclose Personal Data to Sub-processors that are parties to written agreements with RSSBUS including obligations no less protective that the obligations of this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor. Customer agrees to enter into the Standard Contractual Clauses set out in Attachment 1 to the extent necessary and acknowledges that Sub-processors may be appointed by RSSBUS in accordance with Clause 11 of Attachment 1.

5.2. List of Current Sub-processors and Notification of New Sub-processors. A current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location is attached hereto on Appendix 3 of Attachment 1 ("**Sub-processor List**"). Customer may receive notifications of new Sub-processors by emailing gdpr@RSSBUS.com with the subject "Subscribe" and the appropriate contact information included in the body of the email, and if a Customer contact subscribes, RSSBUS shall provide the subscriber with notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Software and/or Services.

5.3. Objection Right for New Sub-processors. Customer may reasonably object to RSSBUS' use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or decrease protections for such Personal Data) by notifying RSSBUS promptly in writing within ten (10) business days after receipt of RSSBUS' notice in accordance with the mechanism set out in Section 5.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, RSSBUS will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If RSSBUS is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate the applicable Order(s) with respect only to those aspects of the Services which cannot be provided by RSSBUS without the use of the objected-to new Sub-processor by providing written notice to RSSBUS. RSSBUS will refund Customer any prepaid fees on a prorated basis of such Order(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. Liability. RSSBUS shall be liable for the acts and omissions of its Sub-processors to the same extent RSSBUS would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY; AUDIT RIGHTS

6.1. Controls for the Protection of Personal Data. RSSBUS will maintain appropriate technical and organizational safeguards against unauthorized or unlawful Processing of the Personal Data, and against accidental loss or destruction of, and damage to the Customer Data, according to the measures set forth on Appendix 2 of Attachment 1. RSSBUS' obligations under this Section 6.1 will be satisfied by complying with terms of such Appendix 2 of Attachment 1.

6.2. Audit Rights. RSSBUS will allow Customer to perform an on-site audit of RSSBUS, at Customer's sole expense, for compliance with the technical and organizational measures set forth in the Appendix 2 of Attachment 1 if (i) RSSBUS notifies Customer of a Security Incident, or (ii) if Customer reasonably believes that RSSBUS is not in compliance with its security commitments under this DPA, or (iii) if such audit legally is required by Customer's Applicable Laws. Such audit must be conducted in accordance with the procedures set forth in Section 6.5 and may not be conducted more than one time per year.

6.3. Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, RSSBUS may satisfy such audit request by providing Customer with a confidential copy of an Audit Report (described in Section 6.2) in order that Customer may reasonably verify RSSBUS' compliance with the technical and organizational measures set forth in Appendix 2 of Attachment 1.

6.4. Audit Process. Customer must provide at least 6 weeks' prior written notice to RSSBUS of a request to audit. The scope of any audit will be limited to RSSBUS' policies, procedures and controls relevant to the protection of Customer Data and defined in Appendix 2 of Attachment 1. All audits will be conducted during normal business hours, at RSSBUS' principal place of business or other location(s) where Customer Data is accessed, processed or administered, and will not unreasonably interfere with RSSBUS' day-to-day operations. An audit will be conducted at Customer's sole cost and by a mutually agreed upon third party contractor who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all RSSBUS Confidential Information and all audit findings. Before the commencement of any such on-site audit, RSSBUS and Customer shall mutually agree upon the timing, and duration of the audit and in addition RSSBUS will provide RSSBUS' reimbursement rate for which Customer shall be responsible (RSSBUS' then-current professional Software and/or Services rates). RSSBUS will co-operate with the audit, including providing auditor the right to review but not to copy RSSBUS security information or materials. RSSBUS' policy is to share methodology, and executive summary information, not raw data or private information. Customer shall, at no charge, provide to RSSBUS a full copy of all findings of the audit.

6.5. Notice of Failure to Comply. After conducting an audit under Section 6.3 or after receiving a RSSBUS Report under Section 6.4, Customer must notify RSSBUS of the specific manner, if any, in which RSSBUS does not comply with any of the security, confidentiality, or data protection obligations in this DPA, if applicable. Any such information will be deemed Confidential Information of RSSBUS. Upon such notice, RSSBUS will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION.

7.1. RSSBUS shall notify Customer of any breach relating to Personal Data (within the meaning of applicable Data Protection Laws and Regulations) of which RSSBUS becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under applicable Data Protection Law and Regulations (a "**Customer Data Incident**"). RSSBUS shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as RSSBUS deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within RSSBUS' reasonable control. The obligations herein shall not apply to incidents that are caused by Customer, Customer's end users, or any services or software not provided by RSSBUS.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1. Upon termination of the Agreement for which RSSBUS is Processing Personal Data, RSSBUS shall, upon Customer's request, and subject to the limitations described in the Agreement return all Customer Data and copies of such data to Customer or securely destroy them and demonstrate to the reasonable satisfaction of Customer that it has taken such measures, unless the retention of such data is requested by Customer or mandated by applicable law. RSSBUS agrees to preserve the confidentiality of any retained Customer Data and will only actively Process such Customer Data after such termination date in order to comply with the laws to which it is subject.

9. DATA PROTECTION IMPACT ASSESSMENT

9.1. Upon Customer's request, RSSBUS shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is

available to RSSBUS. RSSBUS shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.2, to the extent required under the GDPR.

10. LIMITATION OF LIABILITY

10.1. 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 Authorized Affiliates and RSSBUS, 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.

10.2. For the avoidance of doubt, RSSBUS' and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including Attachment 1 and Appendices 1-3.

11. TRANSFER MECHANISM FOR DATA TRANSFERS.

11.1. For any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations, the Standard Contractual Clauses set forth in Attachment 1 and Appendices 1-3 to this DPA shall apply.

12. LEGAL EFFECT; TERMINATION

12.1. This DPA shall only become legally binding between Customer and RSSBUS when fully executed and will terminate when the Agreement terminates, without further action required by either party.

13. CONFLICT

13.1. In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA will prevail.

IN WITNESS WHEREOF, the parties have caused this Data Processing Addendum to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below are on the date of signature duly authorized.

On behalf of the Customer: _____	**On behalf of RSSBUS LLC.:**
Name (written out in full): _____	Name (written out in full): Kathy L. Priest
Position: _____	Position: General Counsel
Address: _____ _____	Address: 101 Europa Drive, Suite 110, Chapel Hill, North Carolina 27517 USA
Signature: _____	Signature: Kathy L. Priest

Attachment 1

EU Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: ..... ; fax: ..... ; e-mail: .....

(the data **exporter**)

And

Name of the data importing organisation: RSSBUS LLC.

Address: 101 Europa Drive, Suite 110, Chapel Hill, North Carolina 27517 USA

Tel.:1-800-743-8232; fax: 1-415-358-4669; e-mail: legal@RSSBUS.com

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) 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 specified in Appendix 1.

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 sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exp*orter*.

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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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[3], with the consent of the data exporter, 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 data importer under the Clauses1. Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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 sub-processor 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 sub-processor 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.

On behalf of the data exporter:

On behalf of: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

On behalf of RSSBUS LLC.:

Name (written out in full): Kathy L. Priest

Position: General Counsel

Address: 101 Europa Drive, Suite 110

Chapel Hill, North Carolina 27517 USA

Signature: Kathy L. Priest

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Using the Services as described in the Agreement.

Data importer

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

Providing the Services as described in the Agreement.

Data subjects

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

The data exporter may submit Personal Data to the data importer as part of the Customer Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors (who are natural persons)
- Employees, agents, advisors, consultants of Customer (who are natural persons)

Categories of data

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

The data exporter may submit Personal Data to the data importer as part of the Customer Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data: Customer's identification and contact data (name, email address, address, title, contact details, username); employment details (employer, job title, geographic location, area of responsibility); IP address, cookie data and other data collected via automated means from users of websites or apps, such as clickstream data.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

The parties do not anticipate the transfer of special categories of data.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by the data importer is the delivery of the Services pursuant to the Agreement.

On behalf of the data exporter:	**On behalf of the data importer:**
On behalf of: _____	On behalf of RSSBUS LLC.:
Name (written out in full): _____	Name (written out in full): Kathy L. Priest
Position: _____	Position: General Counsel
Address: _____	Address: 101 Europa Drive, Suite 110
	Chapel Hill, North Carolina 27517 USA
Signature: _____	Signature: Kathy L. Priest

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

The data importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material degradation in the security of the Services during the term of the Agreement.

RSSBUS shall implement and maintain an written information security management policy with standards that are no less rigorous than accepted industry practices, comply with all applicable law to protect the personal data from loss or unauthorized access, destruction, use, modification, disclosure or other Processing, as well as comply with the provisions of this Appendix 2. Consistent with this policy, RSSBUS shall implement physical, technical, and administrative information safeguards that adequately provide for: (a) protection of business facilities, paper files, servers, computing equipment, including all mobile devices and other equipment with information storage capability, and backup systems containing the personal data; (b) network, application (including databases), and platform security; (c) business systems designed to optimize security; (d) secure, encrypted transmission and secure, encrypted storage of personal data; (e) authentication and access control mechanisms; and (f) personnel security, including recent strong background checks on all such personnel to the extent permitted by law, use of unique, robust passwords, and annual training on how to comply with RSSBUS' physical, technical, and administrative information security safeguards.

RSSBUS shall regularly test and monitor the effectiveness of its security practices and procedures relating to the personal data and will evaluate and adjust its information security program in light of the results of the testing and monitoring, any relevant changes to its operations or business arrangements, or any other circumstances that RSSBUS knows or reasonably should know may have a material effect on the effectiveness of its information security program.

Without limiting the foregoing, RSSBUS shall implement the following security controls:

1. <u>Admittance Control (physical):</u>
   - RSSBUS will prevent unauthorised persons from gaining access to the systems used to process personal data.
   - RSSBUS will protect offices in which personal data is processed against access by unauthorized persons.

2. <u>Entry Control (systems):</u>
   - RSSBUS will prevent data processing systems from being used without authorisation.
   - RSSBUS will only grant the personnel of RSSBUS and its permitted subprocessors access to applications that process personal data to the extent they require it to fulfill their function.
   - RSSBUS will ensure that the entry control is supported by an authentication system that includes regular, iterated grant checks.
   - RSSBUS shall conduct appropriate systems hardening, including appropriate intrusion detection and network-level isolation.

3. <u>Access Control (data):</u>
   - RSSBUS will ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access (including in QA, staging and live systems), and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or after storage.
   - RSSBUS will enforce password complexity rules and other brute force protection methods on its personnels' accounts on appropriate systems.
   - RSSBUS will grant authorisation to access personal data only to personnel who need the access to perform their functions. Additionally, RSSBUS will only grant the personnel the level of access (e.g., roles) required by such personnel to perform their respective functions. RSSBUS will ensure that only authorised RSSBUS personnel can access the personal data.
   - RSSBUS also shall provide user management features to Customer. For example, the RSSBUS account owner shall be able to assign different roles and permissions to account users.

4. Transfer Control:

- RSSBUS will ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which parties the transfer of personal data is envisaged.
- RSSBUS will encrypt all personal data if it is stored in an environment without physical access control or if it is stored or transferred outside RSSBUS' logical and physical access control system.
- RSSBUS will encrypt data while transferred through internal or external networks, including between RSSBUS data centers. For example, all data transfers between an end user and the RSSBUS platform that the user has logged into are encrypted.
- Communications between data centers shall be secured and encrypted for all connections, including, management, control, backup and replication data flows.

5. Input Control:

- RSSBUS will ensure that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed.
- RSSBUS may permit only authorised personnel to modify any personal data within the scope of their function.
- RSSBUS must record any changes made to the personal data, if not made by Customer.
- This will be achieved by means of logging of system access events, console events, and user-issued commands.

6. Job Control:

- RSSBUS will carry out the services and, in particular, the data processing services, for Customer only in accordance with Customer's instructions as set forth in the Addendum.

7. Availability Control:

- RSSBUS will protect personal data against accidental destruction or loss.
- RSSBUS will implement measures that enable RSSBUS to resume the services within a commercially reasonable timeframe if there is a breakdown of the services.
- Safeguards include Regular backups and Disaster recovery testing at least annually

8. Purpose Separation:

- RSSBUS will ensure that personal data collected for different purposes can be processed separately.

9. Security Incident Protection:

- A "**Security Incident**" is any reasonably suspected or actual loss of or unauthorized processing of personal data.
- Unless prohibited by law, RSSBUS will immediately (but in no event later than 24 hours after discovery) notify the data exporter of any actual or suspected Security Incident or privacy or security-related complaint relating to the personal data or the services provided by RSSBUS. Such disclosure shall describe the incident, the suspected effect on the data exporter, its personal data and affected individuals, RSSBUS' actual and anticipated corrective action to respond to the incident, and (if possible) the outcome of the incident. RSSBUS shall provide at least daily updates of this information as new information emerges.
- RSSBUS also shall take immediate steps to investigate, remedy and mitigate the harm caused by the Security Incident at RSSBUS' expense. Without limiting the foregoing, RSSBUS shall permit an independent qualified third party auditor to perform an investigation (including the installation of monitoring or diagnostic software or equipment) to locate the source and scope of the breach and provide the data exporter with any material information related to the data exporter that such independent auditor discovers with respect to the incident.
- Except as may be strictly required by applicable law, RSSBUS agrees that it will not inform any third party of any such Security Incident without first obtaining the data exporter's prior written consent, other than to inform affected individuals who inquire about the incident that their inquiry has been forwarded to the data exporter's legal department. If, however, such disclosure is, in the opinion of legal counsel, required by applicable law, the parties agree to work with each other regarding the content of such disclosure so as to minimize any potential adverse impact upon the data exporter and on any individuals whose personal data was involved in the Security Incident.

- RSSBUS shall immediately notify the data exporter of any investigations of its information use or privacy or information security practices or Security Incident by a governmental, regulatory, or self-regulatory organization.

On behalf of the data exporter:

On behalf of: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

On behalf of RSSBUS LLC.:

Name (written out in full): Kathy L. Priest

Position: General Counsel

Address: 101 Europa Drive, Suite 110

Chapel Hill, North Carolina 27517 USA

Signature: Kathy L. Priest

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The list of sub-processors approved by the data importer as of the effective date of the DPA is as set forth below:	Description and Location of Processing
Google, Inc.	Data analytics – USA
HubSpot, Inc.	Cloud hosting and storage services; Online marketing services – USA
Amazon Web Services	Data hosting provider - USA
The Rocket Science Group LLC d/b/a MailChimp	Content delivery and review services - USA
Digital Ocean	E-mail hosting provider - USA

On behalf of the data exporter:

On behalf of: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of the data importer:

On behalf of RSSBUS LLC.:

Name (written out in full): Kathy L. Priest

Position: General Counsel

Address: 101 Europa Drive, Suite 110

Chapel Hill, North Carolina 27517 USA

Signature: Kathy L. Priest