NETROADSHOW

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**DPA**") forms part of the NetRoadshow Master Services Agreement (the "**Principal Agreement"**) by and between NetRoadshow, Inc. on its own behalf and on behalf of its Affiliates ("**NRS**") and _____ (the "**Customer**") and is subject to the Principal Agreement.

1. Definitions. For the purposes of this DPA, capitalized terms shall have the following meanings. Capitalized terms not otherwise defined shall have the meaning given to them in the Principal Agreement.

(a) "**Affiliates**" means any entity that is owned or that owns NRS or that is under common control with one of NRS's entities.

(b) "**Customer's Personal Data**" means any personal data that is processed by NRS on behalf of the Customer to perform the Services under the Principal Agreement.

(c) "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (with effect from May 25, 2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

(d) "**GDPR**" means EU General Data Protection Regulation 2016/679.

(e) "**EEA**" means the European Economic Area.

(f) "**NRS Infrastructure**" means (i) NRS physical facilities; (ii) hosted cloud infrastructure; (iii) NRS's corporate network and the non-public internal network, software, and hardware necessary to provide the Services and which is controlled by NRS; in each case to the extent used to provide the Services.

(g) "**Restricted Transfer**" means a transfer of the Customer's Personal Data from NRS to a sub-processor where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws) in the absence of appropriate safeguards required for such transfers under EU Data Protection Laws.

(h) "**Services**" means the services provided to the Customer by NRS pursuant to the Principal Agreement.

(i) "**Standard Contractual Clauses**" means the latest version of the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (the current version as at the date of this DPA is annexed to European Commission Decision 2010/87/EU).

(j) The terms "**consent**", "**controller**", "**data subject**", "**Member State**", "**personal data**", "**personal data breach**", "**processor**", "**sub processor**", "**processing**", "**supervisory authority**" and "**third party**" shall have the meanings ascribed to them in article 4 of the GDPR.

2. Compliance with EU Data Protection Laws

(a) NRS and the Customer shall each comply with the provisions and obligations imposed on them by the EU Data Protection Laws and shall procure that their employees, agents and contractors observe the provisions of the EU Data Protection Laws.

3. Details and Scope of the Processing

(a) The Processing of the Customer's Personal Data within the scope of the Agreement shall be carried out in accordance with the following stipulations and as required under Article 28(3) of the GDPR. The parties may amend this information from time to time, as the parties may reasonably consider necessary to meet those requirements.

(i) **Subject matter and duration of the processing of Personal Data:** The subject matter and duration of the processing of the Personal Data are set out in the Services orders.

(ii) **The nature and purpose of the processing of Personal Data:** Under the Principal Agreement, NRS provides certain services to the Customer which involves the processing of personal data. Such processing activities include (a) providing the Services; (b) the detection, prevention and resolution of security and technical issues; and (c) responding to Customer's support requests.

(iii) **The types of Personal Data to be processed:** The personal data submitted, the extent of which is determined and controlled by the Controller in its sole discretion, includes name, email, telephone numbers IP address and other personal data included in the contact lists and message content.

(iv) **The categories of data subject to whom the Personal Data relates:** Senders and recipients of email and telephone numbers.

(b) NRS shall only process the Customer's Personal Data (i) for the purposes of fulfilling its obligations under the Principal Agreement and (ii) in accordance with the documented instructions described in this DPA or as otherwise instructed by the Customer from time to time. Such Customer's instructions shall be documented in the applicable order, services description, support ticket, other written communication or as directed by Customer using the Services.

(c) Where NRS reasonably believes that a Customer instruction is contrary to the provisions of the Principal Agreement or this DPA, or that it infringes the GDPR or other applicable data protection provisions, it shall inform the Customer without delay. In both cases, NRS shall be authorized to defer the performance of the relevant instruction until it has been amended by Customer or is mutually agreed by both Customer and NRS.

(d) Customer is solely responsible for its utilization and management of Personal Data submitted or transmitted by the Services, including: (i) verifying recipient's addresses and that they are correctly entered into the Services (ii) reasonably notifying any recipient of the insecure nature of email as a means of transmitting Personal Data (as applicable), (iii) reasonably limiting the amount or type of information disclosed through the Services (iv) encrypting any Personal Data transmitted through the Services where appropriate or required by applicable law (such as through the use of encrypted attachments, PGP toolsets, or S/MIME). When the Customer decides not to configure mandatory encryption, the Customer acknowledges that the Services may include the transmission of unencrypted email in plain text over the public internet and open networks. Information uploaded to the Services, including message content, is stored in an encrypted format when processed by the NRS Infrastructure.

4. Controller and Processor

(a) For the purposes of this DPA, the Customer is the controller of the Customer's Personal Data and NRS is the processor of such data, except when the Customer acts as a processor of the Customer's Personal Data, in which case NRS is a sub-processor.

(b) NRS shall at all times have in place an officer who is responsible for assisting the Customer (i) in responding to inquiries concerning the Data Processing received from Data Subjects; and, (ii) in completing all legal information and disclosure requirements which apply and are associated with the Data Processing. The Data Protection Officer may be contacted directly at security@NRS.com.

(c) The Customer warrants that:

(i) The processing of the Customer's Personal Data is based on legal grounds for processing, as may be required by EU Data Protection Laws and that it has made and shall maintain throughout the term of the Principal Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by EU Data Protection Laws with respect to NRS's processing of the Customer's Personal Data under this DPA and the Principal Agreement;

(ii) it is entitled to and has all necessary rights, permissions and consents to transfer the Customer's Personal Data to NRS and otherwise permit NRS to process the Customer's Personal Data on its behalf, so that NRS may lawfully use, process and transfer the Customer's Personal Data in order to carry out the Services and perform NRS's other rights and obligations under this DPA and the Principal Agreement;

(iii) it will inform its Data Subjects about its use of Processors in Processing their Personal Data, to the extent required under applicable EU Data Protection Laws; and,

(iv) it will respond in a reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data, and to give appropriate instructions to the Processor in a timely manner.

5. Confidentiality

(a) NRS shall ensure that each of its, and sub-processors', personnel that is authorized to process the Customer's Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality and are trained with the relevant security and Data Protection requirements.

6. Technical and Organizational Measures

(a) NRS shall, in relation to the Customer's Personal Data, (a) take and document, as appropriate, reasonable and appropriate measures required pursuant to Article 32 of the GDPR in relation to the security of the NRS Infrastructure and the platforms used to provide the Services as described in the Principal Agreement, and (b) on reasonable request at the Customer's cost, assist the Customer in ensuring compliance with the Customer's obligations pursuant to Article 32 of the GDPR.

(b) NRS's internal operating procedures shall comply with the specific requirements of an effective Data Protection management.

7. Data Subject Requests

(a) NRS provides specific tools in order to assist customers in replying to requests received from data subjects. When NRS receives a complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to EU Data Protection Laws) related to the Customer's Personal Data directly from data subjects NRS will notify the Customer within 14 days from the receipt of the complaint, inquiry or request. Taking into account the nature of the processing, NRS shall assist the Customer at the Customer's cost, by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of the Customer's obligation to respond to requests for exercising such data subjects' rights.

8. Personal Data Breaches

(a) NRS shall notify the Customer without undue delay once NRS becomes aware of a personal data breach affecting the Customer's Personal Data. NRS shall, taking into account the nature of the processing and the information available to NRS, use commercially reasonable efforts to provide the Customer with sufficient information to allow the Customer at the Customer's cost, to meet any obligations to report or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required under EU Data Protection Laws.

9. Data Protection Impact Assessments

(a) NRS shall, taking into account the nature of the processing and the information available, provide reasonable assistance to the Customer at the Customer's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Customer to fulfill its obligations under EU Data Protection Laws.

10. Audits

(a) NRS shall make available to the Customer on reasonable request, information that is reasonably necessary to demonstrate NRS' compliance with this DPA.

(b) Customer, or a mandated third party auditor, may upon written reasonable request conduct an inspection in relation to the Processing of the Customer's Personal Data by NRS and to the extent necessary according to Data Protections Laws and without interrupting NRS's business operations and ensuring confidentiality. The Customer shall be responsible for any costs and expenses of Processor arising from the provision of such audit rights.

11. Return or Destruction of the Customer's Personal Data

(a) The Customer may, by written notice to NRS, request the return and/or certificate of deletion of all copies of the Customer's Personal Data in the control or possession of NRS and sub-processors. NRS shall provide a copy of the Controller's Data in a form that can be read and processed further.

(b) Within ninety (90) days following termination of the Principal Agreement, the Processor shall delete and/or return all Personal Data processed pursuant to this DPA. This provision shall not affect potential statutory duties of the Parties to preserve records for retention periods set by law, statute or contract. NRS may retain electronic copies of files containing Customer's Personal Data created pursuant to automatic archiving or back-up procedures which cannot reasonably be deleted. In these cases, NRS shall ensure that the Customer's Personal Data is not further actively processed.

(c) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by the Customer.

12. Data Transfers

(a) Following execution of this DPA, NRS shall, if requested to do so by the Customer and if required by EU Data Protection Laws, enter into the Standard Contractual Clauses as data importer with the Customer acting as data exporter. If NRS's arrangement with a sub-processor involves a Restricted Transfer, NRS shall ensure that the onward transfer provisions of the Standard Contractual Clauses are incorporated into the Principal Agreement, or otherwise entered into, between NRS and the sub-processor. The Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing NRS to conduct the audit set out in Paragraph 10.

(b) Customer acknowledges and agrees that, in connection with the performance of the Services under the Agreement, NRS may transfer Personal Data within its company group. These transfers are necessary to globally provide the Services, and are justified for internal administration purposes.

(c) For transfers of Personal Data 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 of the foregoing territories, to the extent such transfers are subject to Data Protection Laws and Regulations and in order to implement appropriate safeguards, the following safeguards are taken: (i) Standard Contractual Clauses as per European Commission's Decision 2010/87/EU and, (2) additional safeguards with respect to security measures including data encryption and data minimization principles.

13. Sub-processing

(a) The Customer hereby authorizes NRS to appoint sub-processors in accordance with this Paragraph 13 subject to any restrictions in the Principal Agreement. NRS will ensure that sub-processors are bound by written agreements that require them to provide at least the level of data protection required of NRS by this DPA. NRS may continue to use those sub-processors already engaged as at the date of this DPA.

(b) NRS shall give the Customer prior written notice of the appointment of any new sub-processor. If, within ten (10) business days of receipt of that notice, the Customer notifies NRS in writing of any objections on reasonable grounds to the proposed appointment, NRS shall not appoint that proposed sub-

processor until reasonable steps have been taken to address the objections raised by the Customer and the Customer has been provided with a reasonable written explanation of the steps taken. If NRS and the Customer are not able to resolve the appointment of a sub-processor within a reasonable period, either party shall have the right to terminate the Principal Agreement.

(c) In addition, in the event of authorized sub-contracting outside the European Union, the Customer mandates NRS to enter into EU Model Clauses for the specific purposes of the providing the services under the Principal Agreement.

(d) This paragraph does not apply to the following ancillary services, namely telecommunication services, postal or transport services, maintenance and user support tools. NRS shall, however, be obligated to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the Data protection and Data security of the Customer's Data even for these outsourced ancillary services.

(e) NRS shall be responsible for the acts and omissions of any sub-processors as it is to the Customer for its own acts and omissions in relation to the matters provided in this DPA.

14. Governing law and jurisdiction

(a) The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

(b) This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

15. Order of precedence

(a) With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

16. Changes in Data Protection Laws, etc.

(a) NRS may modify or supplement this DPA, with reasonable notice to the Customer:

(i) If required to do so by a supervisory authority or other government or regulatory entity;

(ii) If necessary to comply with applicable law;

(iii) To implement new or updated Standard Contractual Clauses approved by the European Commission; or

(iv) To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR.

17. Severance

(a) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

18. Termination

(a) This DPA and the Standard Contractual Clauses will terminate contemporaneously and automatically with the termination of the Principal Agreement.

(b) NRS may terminate this DPA and the Standard Contractual Clauses if NRS offers alternative mechanisms to Customer that comply with the obligations of the European Union privacy laws for the transfer of Personal Data outside the EEA.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

NetRoadshow, Inc.

Signature: _____

Name:

Title:

Date Signed: _____

The Customer

Signature: _____

Name: _____

Title: _____

Date Signed: _____