GDPR DATA PROTECTION & INFORMATION SECURITY ADDENDUM ("ADDENDUM")

1. Definitions

For the purposes of this Addendum: (i) "**Data Processor**", "**Data Controller**", "**Data Subject**", "**Personal Data**", "**Special Categories of Personal Data**", "**Supervisory Authority**" "**Process**" and "**Processing**" shall have the same meaning as set out in Article 4 of the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"); (ii) "**Relevant Data**" means Contact Information, as defined in the Agreement and any other non-public data collected, held, or processed by or on behalf of a data controller, regardless of the form, whether electronic or physical; (iii) "**Data Protection Laws**" means any data protection laws or regulations applicable to Processing of Personal Data contemplated by the agreement or regulations in which this Addendum is included (the "**Agreement**"), including, without limitation, applicable U.S. laws, Directive 95/46/EC and any related decisions or guidelines and subsequent legislation of a similar nature, and in particular the GDPR; (iv) "**InfoSecurity**" is the practice of preventing unauthorized access, use, disclosure, disruption, denial of access, modification, inspection, recording or destruction of information, regardless of the form; (v) "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data from the European Union/European Economic Area to Data Processors established in third countries (Data Controller-to-Data Processor transfers), as set out in the Annex to Commission Decision 2010/87/EU; (vi) "**Top 10 Risks**" are set out in the Open Web Application Security Project - (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project); and (vii) "**IT System(s)**" means any IT system of a Data Processor used under the Agreement. In the event of any conflict or inconsistency between the terms and conditions of this Addendum and the Agreement, the terms of this Addendum shall prevail. For the purposes of this Addendum, AAPEX Show Management shall be deemed a Data Controller and the Exhibitor shall be deemed a Data Processor, for the purposes of the AAPEX Exhibitor Regulations.

2. Security of Data

2.1 The Data Processor will implement appropriate technical and organizational measures to ensure against unauthorized or unlawful access, use, disclosure, processing or modification and accidental loss, destruction of or damage to Relevant Data in Data Processor's possession or control (e.g. Relevant Data 'in flight' from any IT System under the control of Data Processor or its authorized vendor or at rest in any such IT System, will be encrypted and interfaces between IT Systems will use strong credentials and authentication). Security information will never be sent in the clear and administrative privileges will only be shared on a "need-to-know" basis. Logical and physical security of servers and other computer resources will be assured. Relevant Data not needed at present will not be retained and will be retained for the shortest possible time, subject to Data Processor's legal obligations. Data storage must be identified geographically. Any IT System shall protect against the Top 10 Risks.

2.2 The Data Processor will implement commercially reasonable (but no less stringent than as required by applicable law) practices and protections against any virus and internet attacks, not compromise security by functionality changes, patch IT Systems to prevailing industry practices and keep code libraries up-to-date. The Data Processor's IT Systems will achieve satisfactory test status by the Data Controller for all releases to the production environments, use a deployment process that ensures authority and efficacy of any release (including rollback and failed release planning) and maintain skilled staff or contractors to ensure IT Systems are appropriately supported at all times.

2.3 Upon reasonable notice, the Data Processor will allow the Data Controller (or a Data Controller appointed third party representative), to review and audit Data Processor's information handling practices to ensure the Data Processor's compliance with the terms of this Addendum.

3. Data Processor's Obligations

3.1 The Data Processor must at all times Process any Personal Data held in connection with the Agreement in accordance with all applicable Data Protection Laws and only for the purposes of fulfilling its obligations under the Agreement and under the relevant Data Controller's instructions contemplated or set forth in the Agreement and shall not Process Personal Data for any other purpose.

3.2 If Data Processor becomes aware of: (a) any breach of this Addendum by the Data Processor; (b) an actual or attempted breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Relevant Data transmitted, stored or otherwise processed; (c) any act or practice of Data Processor, its employees or its subcontractors which causes or may reasonably be believed to cause a failure by or inability of a Data Controller to comply with its obligations under the Data Protection Laws or any privacy statements or policies issued by it; or (d) any breach of any of the Data Protection Laws that apply directly to Data Processor and its duties and obligations under the Agreement, then, the Data Processor must take appropriate actions to contain, investigate, mitigate, recover, restore, and notify the Data Controller as soon as is reasonably practicable (but in all circumstances, within no more than twelve hours following the discovery or knowledge of any of the foregoing) of that act or omission. To the extent then known by the Data Processor, the data breach notification shall contain a description of the nature of the data breach including the categories and approximate number of Data Subjects affected, categories of Personal Data affected, date and time, technical and organizational security measures taken to cure the breach, and if applicable, other(s) Data Processor(s) involved and a description of the likely consequences of the data breach and description of any corrections or remedial action taken. The Data Processor, at its own cost, will provide commercially reasonable and any legally required cooperation and assistance to the Data Controller in meeting any investigative, remedial, notification and other requirement(s) under applicable Data Protection Laws or as may be reasonably necessary for the Data Controllers to meet their obligations as a data controller.

3.3 In the event that the Data Processor receives any request or notice from a Supervisory Authority or Data Subject, relating to the services provided by and the obligations of Data Processor under the Agreement, the Data Processor will notify the Data Controller as soon as is commercially practicable (but in all events within no more than twelve hours following receipt of such request or notice) and assist the Data Controller promptly with such requests.

3.4 Without the prior written approval of the Data Controller or as expressly permitted under the Agreement, the Data Processor shall not allow any third party to access, transfer or process Relevant Data. The third party's processing and data use activities shall be governed by no less restrictive provisions than the provisions set out in this Addendum.

3.5 Transfers of Personal Data from the European Economic Area, Switzerland, and UK to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws may be permitted only if advance written notice is provided to the Data Controller and appropriate safeguards are put in place. Such safeguards may include entering into Standard Contractual Clauses without any additions, modifications, or omissions or any other GDPR-compliant safeguards. The Parties acknowledge and agree that transfers may be made to the United States, provided the recipient organization is certified under the EU-US Privacy Shield Framework.

3.6 As soon as is commercially practicable, on termination or expiration of the Agreement, or upon request by the Data Controller, the Data Processor must, at the Data Controller's election return all Relevant Data or destroy all such Relevant Data, in a manner consistent with the GDPR. If the relevant law binding

on the Data Processor prevents it from doing as requested, the Data Processor hereby agrees that it will continue to observe the terms of this Addendum for as long as it is required to retain such Relevant Data. Once no longer required to retain such Relevant Data, the Data Processor will destroy the Relevant Data and certify such destruction to the Data Controller.

4. Privacy and Information Security Impact Assessments

4.1 Upon request, the Data Processor will assist the Data Controller in ensuring compliance with the obligation to conduct vendor assessments and data protection impact assessments of Data Processor's activities under the Agreement.

4.2 The Data Processor shall create and maintain a record of its Processing activities as reasonably requested to support the Data Controllers' obligations under the GDPR, including, without limitation under Article 30 of the GDPR.

5. Audit

Upon reasonable request by the Data Controller, the Data Processor shall at its own cost make available to the Data Controller or its auditor all information and access reasonably necessary to assess the Data Processor's compliance with the obligations of this Addendum.

6. Data Processing Information

6.1 The subject-matter of Processing of Personal Data by the Data Processor is the performance of the Services pursuant to the Agreement:

a. **Nature and purpose of the Processing: The** Data Processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Agreement, and as further instructed by the Data Controller as contemplated in the Agreement, including this Addendum. No processing of Data Controller Data shall be undertaken by the Data Processor except pursuant to the written agreement of the Data Processor and the Data Controller or its authorized representative;
b. **Duration of the processing:** The Data Processor will Process the Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing;
c. **Categories of Data Subjects:** The Data Subjects are as described in the Agreement;
d. **Types of Personal Data:** The types of Personal Data to be Processed are as described in the Agreement and may include, but is not limited to, name, job title, employer, contact information, ID data, personal life data, mobile data, connection data, or localization data.

6.2 The parties are required to keep the above information up-to-date. The Data Controller will notify the Data Processor in writing of any change in any of the foregoing. Any request by the Data Processor to materially modify or amend the matters set forth in section 6.1, shall be in writing to the Data Controller or its authorized representative and shall be subject to the written consent of the Data Controller or its authorized representative.

7. Indemnity

The Data Processor agrees to indemnify and keep indemnified, and defend at its own expense, the Data Controller against all costs, claims, damages or expenses incurred by any Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor, its employees, agents or sub-contractors to comply in all material respects with any of its obligations under this Addendum. Any limitations of liability contained in the Agreement shall not apply to a breach of this Addendum.