DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**DPA**") is a binding legal agreement between [Pegasus Business Intelligence, LP d/b/a Onyx CenterSource] (together with its affiliates and/or other companies of Onyx Group, "**Onyx**") and the customer ("**Customer**") that agrees to any order, terms and conditions (including Onyx's standard online terms and conditions for its hotel and agency customers), or other agreement that references this DPA (the "**Agreement**").Onyx´s Privacy Policy is available at https://www.onyxcentersource.com/privacy-policy/

DEFINITIONS; INTERPRETATION

Unless otherwise specified below or herein, all capitalized terms used in this Data Processing Addendum shall have the same meaning as stated in the Agreement:

"**EEA**" means the European Economic Area;

"**Data Incident**" means a known or reasonably suspected unauthorized or unlawful access to, disclosure, modification, destruction, deletion, loss of, or disruption or loss of access to Controller Personal Data;

"**Data Laws**" means any applicable laws regarding data privacy, including (as applicable and without limitation) the GDPR;

"CCPA" Addendum means the California Consumer Privacy Act Addendum which is made up of the Addendum at Schedule 1 hereto.

"**GDPR**" means (i) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**") as implemented by countries within the EEA; and (ii) the EU GDPR as retained as law in England and Wales by the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), in each case as applicable to the processing;

"**Personal Data**" means any information made available by Customer to Onyx that (i) can be used, alone or in connection with other information, to identify an individual; or (ii) is otherwise subject to any Data Laws;

"**Process**," "**Processed**" or "**Processing**" means any operation or set of operations that are performed on Personal Data or on sets of Personal Data, including by automated means, and pursuant to the instructions set forth herein;

"**Restricted Transfer**" means (a) a transfer of Personal Data from or which originated in the EEA to a Third Country that is not considered to provide an "adequate level" of data protection by the European Commission and where such transfer is subject to the EU GDPR ("**EEA Restricted Transfer**"); or (b) a transfer of Personal Data from or which originated in the UK to a Third Country that is not considered to provide an "adequate level"

of data protection by the UK Government and where such transfer is subject to the UK GDPR ("**UK Restricted Transfer**");

"**Standard Contractual Clauses**" means the standard contractual clauses available at https://www.onyxcentersource.com/ec-standard-contractual-clauses/

"**Third Country**" means a country outside of the EEA, and the UK (as applicable); and

"**UK Addendum**" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses available at https://www.onyxcentersource.com/ec-standard-contractual-clauses/.

To the extent that:

(a) the terms contained in this Data Processing Addendum conflict with those contained in the Agreement, the terms in this Data Processing Addendum shall prevail to the extent the conflict relates to the processing of Personal Data which is subject to Data Laws;

(b) the terms contained in this Data Processing Addendum conflict with those contained in the Standard Contractual Clauses the terms in the Standard Contractual Clauses shall prevail to the extent the conflict relates to a Restricted Transfer; and

(c) the terms contained in the UK Addendum conflict with those in the Standard Contractual Clauses, the terms in the UK Addendum shall prevail in accordance with the hierarchy provisions therein to the extent the conflict relates to a UK Restricted Transfer.

GENERAL

Purpose. Customer has requested Onyx to provide certain services as further described and agreed in the Agreement. Onyx requires access to certain Personal Data on behalf of the Customer in order to be able to fulfill its obligations and provide the services under the Agreement.

Roles. Customer is responsible for determining the purposes and means of processing of the Personal Data. Customer is the "Controller" and Onyx the "Processor", as those terms are used in applicable Data Laws. Customer represents and warrants that it has obtained any necessary consents and authorizations required under Data Laws, and is otherwise fully entitled to transmit any Personal Data to Onyx, all for purposes of processing pursuant to the Agreement. Each party will comply with all applicable Data Laws.

Scope and Instructions. Onyx will process the Personal Data only on and in accordance with Customer's documented instructions. The parties agree and acknowledge that the Agreement constitutes Customer's instructions as to the subject matter, type of Personal Data, and duration of processing to be provided by Onyx pursuant thereto. To the extent permitted by law, Onyx will promptly inform Customer of any legal requirement that would require Onyx to process the Personal Data other than pursuant to Customer's documented

instructions, or if Onyx believes Customer's instructions violate any Data Laws.

Security. Onyx shall implement and maintain appropriate technical and organizational measures in relation to the processing of Personal Data, such that the processing will meet the requirements of Data Laws. For purposes of this section, "appropriate" means commercially reasonable based on an assessment of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Subprocessors. Onyx shall not engage a subprocessor to perform specific processing activities in respect of the Personal Data on behalf of Customer without prior written consent of Customer and, if Customer gives its consent, Onyx shall appoint the subprocessor under a binding written contract which imposes the same data protection obligations as are contained in this DPA. Customer hereby expressly authorizes Onyx to engage subprocessors for provision of technological services and maintenance of systems (between others, data hosting) that facilitate Onyx's provision of its services generally across its customer base (including, but not specifically for, Customer). Onyx will notify Customer, through the Legal Notice in the Onyx Network, about any change in its subprocessors, giving Customer an opportunity to object to any changes. Onyx will use commercially reasonable efforts to address any such objections, but the parties agree and acknowledge that Onyx may be unable to accommodate requests from any one customer as relates to Onyx's uniform provision of the services across its customer base as a whole.

Personnel. Onyx shall ensure that its personnel processing Personal Data have signed agreements requiring them to keep Personal Data confidential or are under an appropriate statutory obligation of confidentiality. Onyx shall ensure that its personnel processing Personal Data have received formation about Personal Data protection.

Assistance. Taking into account the nature of the processing under the Agreement, Onyx shall implement and maintain appropriate technical and organizational measures to assist Customer, insofar as this is possible, in the fulfilment of Customer's obligations to respond to data subject requests for exercising any right of the data subject under Data Laws. Onyx will ensure that all data subject requests it receives are recorded and referred to Customer. Onyx shall provide reasonable assistance, information and cooperation to Customers to facilitate Customer's compliance with its obligations under Data Laws. Customer will, at Onyx's request, reimburse Onyx at reasonable rates for any time spent and costs incurred in providing such cooperation to the Customer in the event of requests which are manifestly unfounded or excessive, in particular because of their repetitive nature.

Records. Onyx shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of Customer containing such information as required under Data Laws ("

Processing Records"), and shall make available to Customer on request in a timely manner such information (including the Processing Records) as is reasonably required by Customer to demonstrate compliance by Onyx with its obligations under Data Laws and this DPA.

Audits. Onyx shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer for the purpose of demonstrating Onyx's compliance with its obligations under Data Laws and this DPA, subject to Customer giving Onyx reasonable prior notice of such audit and/or inspection, ensuring that any auditor is subject to binding obligations of confidentiality, and that such audit or inspection is undertaken at Customer's sole expense and in a manner so as to cause minimal disruption to Onyx's business and other customers. No such audit may take place more than once per twelve months unless otherwise required by Data Laws.

Notification. In respect of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by Onyx under the Agreement, Onyx shall notify Customer of the breach without undue delay and provide Customer without undue delay with available details relating to the breach as Customer reasonably requests.

Destruction. Onyx shall without delay, at Customer's written request, either securely delete or return all the Personal Data to Customer in hardcopy or electronic form after the end of the provision of the relevant services related to processing or, once processing is no longer required for the performance of the Agreement ´s obligations, and securely delete existing copies (unless storage of any data is required by law, in which case Onyx shall notify Customer accordingly).

Language. This DPA is in the English language only, which will be the controlling language with respect to this Agreement in all respects. Any translation of this DPA into another language is for convenience only, and no such translation will be binding against the parties hereto.

State LAWs

To the extent that the services shall involve the processing of California data, the CCPA Addendum at Schedule1 shall apply.

INTERNATIONAL DATA TRANSFERS

EEA Restricted Transfers: To the extent applicable, parties acknowledge and agree that if Customer undertakes an EEA Restricted Transfer to Onyx the parties shall process Personal Data which is subject to the EEA Restricted Transfer in accordance with the Standard Contractual Clauses.

UK Restricted Transfers: The parties acknowledge and agree that if Customer undertakes a UK Restricted Transfer to Onyx the parties shall process Personal Data which is subject to the UK Restricted Transfer in accordance with the Standard Contractual Clauses and the UK Addendum.

The parties acknowledge and agree that to the extent:

(a) Onyx is subject to the requirements of the GDPR with regards the processing of the Personal Data subject to a Restricted Transfer; and

(b) Onyx's obligations in the Standard Contractual Clauses conflict with Onyx's obligations under the GDPR in regard the processing of such Personal Data;

Onyx shall only need to comply with its obligations under the GDPR with regard to such processing.

Module Applicable: The parties acknowledge and agree that Module 2 of the Standard Contractual Clauses applies to the processing.

Amendments: Notwithstanding any restrictions on amendments in the Agreement, the parties acknowledge and agree that should new standard contractual clauses get published (or amendments to the existing Standard Contractual Clauses or UK Addendum) to address Restricted Transfers, and where the parties determine such new or amended clauses are required to address the Restricted Transfers, such new or amended clauses will replace the Standard Contractual Clauses and/or UK Addendum (as applicable) upon notification. All Restricted Transfers will be thereafter made pursuant to such new or amended clauses.

SCHEDULE 1

CALIFORNIA CONSUMER PRIVACY ACT ("CCPA") ADDENDUM

To the extent the CCPA is applicable, the following terms will apply:

PROCESSING RIGHTS AND REQUIREMENTS

General Obligations. Processor will Process Controller Personal Data in compliance with applicable laws, including applicable Data Laws, at all times and in compliance with this DPA. For the purposes of this DPA, Processor is a "service provider," "contractor," or "processor" or similar applicable term defined under applicable Data Law. Processor will not disclose Personal Data to any third party, except pursuant to this DPA.

Scope of the Processing. Processor will Process Controller Personal Data pursuant to the purpose set forth the agreement that references this DPA, and in compliance with this DPA and Data Laws. Processor shall not

Process Controller Personal Data for purposes other than the Specified Purposes set forth in Appendix 1. The Parties agree to abide by the Processing specifications for Controller Personal Data, attached hereto in Appendix 1.

Prohibited Uses. Processor is prohibited from and represents and certifies its understanding that it is prohibited from:

Selling, Sharing, or otherwise disclosing Controller Personal Data to any third party, as such concepts are defined each under applicable Data Laws;

using, retaining, or disclosing Controller Personal Data for any purpose other than the Specified Purpose or engaging a subcontractor in compliance with the DPA, including any other commercial purpose;

using, retaining, or disclosing Controller Personal Data outside of the direct relationship between Controller and Processor;

using, retaining, or disclosing Controller Personal Data against Controller's instructions; and

combining or updating Controller Personal Data with Personal Data received from another source, including Processor's own direct interaction with the consumer, unless expressly permitted applicable law, including applicable Data Laws.

PROCESSING OBLIGATIONS

Processor shall make available to Controller all information necessary to comply with and demonstrate Processor's compliance with Data Laws.

Data Subject Requests.

Processor shall cooperate with, and provide all reasonable support to cause Controller to comply with Controller's obligations to data subjects under Data Laws, including responding to data subject requests. Upon written request from Controller, Processor shall provide necessary information to Controller to fulfill its obligations under Data Laws.

In the event that any individual rights request from a data subject is made directly to Processor concerning Controller Personal Data, Processor shall forward the request to Controller within five (5) calendar days within Processor's receipt of the request. Processor shall not respond to the request without Controller's prior authorization other than to inform the requestor that Processor is not authorized to directly respond to a request and advise that Processor has forwarded the request to Controller.

In the event that any request from applicable legal or regulatory authorities is made directly to Processor, Processor shall promptly forward the request to Controller, no later than five (5) calendar days within Processor's receipt of the request, to the extent legally permitted to do so. Processor shall not respond to such communication directly without Controller's prior authorization other than to inform the requestor that Processor is not authorized to directly respond to a request. If Processor is legally required to directly respond to such a request, Processor will promptly notify Controller and provide it with a copy of the request unless legally prohibited from doing so.

Data Processing Assessments. Processor shall provide information to Controller necessary to enable Controller to conduct and document any data processing or data protection assessments.

Data Retention and Deletion/Return. Processor shall only retain Personal Data for the duration of the agreement that references this DPA, unless a different time period is agreed upon in writing. Except as required under applicable law, upon termination or expiration of the agreement that references this DPA, Processor shall return, delete and/or destroy all Controller Personal Data. Controller shall decide, in its sole discretion, whether Processor shall return or delete Controller Personal Data upon the termination or expiration of the agreement that references this DPA.

Confidentiality. Processor shall ensure that Processor personnel that Process Controller Personal Data keep the Controller Personal Data confidential, are subject to confidentiality obligations that are at least as strict as the requirements Processor has to protect its own confidential information, and are consistent with confidentiality provisions in the agreement that references this DPA. Further,

Processor shall provide information security and data protection or privacy training to its personnel that are Processing Controller Personal Data.

SUB-PROCESSORS

In the event that Processor engages sub-processors to assist it in providing its services to Controller, Processor shall enter into a written agreement with each sub-processor that requires the sub-processor to substantially meet the same terms of this DPA that are applicable to Processor.

AUDITS

Processor grants Controller the right to take reasonable and appropriate steps to ensure that Processor uses Controller Personal Data in a manner consistent with Controller's obligations under the Data Laws. Reasonable and appropriate steps may include assessments of Processor's system(s) and requirements to conduct regular internal or third-party assessments, audits, or other technical or operational testing. Controller will undertake or require such assessments or audits at a reasonable interval, typically once every 12 months, unless there has been a Data Incident or where Controller has evidence-based concerns that Processor is not compliant with the requirements herein.

INFORMATION SECURITY

Processor and Controller shall implement and maintain technical and organizational security measures to protect the security, confidentiality, and integrity of Personal Data and to ensure a level of security appropriate to the risk. Further, Processor must assist in meeting Controller's obligations regarding security of Processing Personal Data, including in relation to notice obligations in a Data Incident. If Processor becomes aware of a Data Incident, it shall promptly (a) notify Controller; (b) provide relevant information, to the extent known, about the Data Incident to Controller; and (c) reasonably cooperate with Controller to support Controller's reasonable reporting and notification obligations.

CERTIFICATION AND NOTIFICATION OBLIGATIONS

Processor certifies that it understands and will comply with the requirements set forth herein. If Processor becomes aware or makes a determination that it can no longer meet its obligations under applicable Data Laws or this DPA, it shall promptly notify Controller.

Appendix 1

The Parties agree that the Processing details are as follows:

(a) Types of Personal Data Processed: Personal Data provided by Controller under the agreement that references this DPA to receive services from Processor.

(b) Nature and Purpose of the Processing: To provide services to Controller ("**Specified Purpose**")

(c) Duration of the Processing: For the duration of the agreement that references this DPA.