Data Security and Privacy Policy Addendum

AOR, Incorporated ("AOR") may, in the course of performing work and services on behalf of the client identified in the applicable scope of work ("Client"), receive, analyze, aggregate or use various pieces of data and information regarding third parties, some of which may be considered personal, sensitive or proprietary by various information privacy laws or regulations, including, without limitation, the California Consumer Privacy Act of 2018 ("CCPA"), and the Global Data Privacy Regulation ("GDPR") (collectively referred to in this Policy as "Data").

The AOR's receipt, access to, or use of the Data is governed by this Data Security and Privacy Policy Addendum (the "Policy"), the provisions of which are incorporated by reference into the Terms and Conditions ("Agreement") and relevant Scope of Work between AOR and Client. Capitalized terms used but not defined in this Policy shall have the meanings set out in the Agreement.

The following definition, as set forth by the CCPA, shall apply to this Policy, the Agreement or relevant Scope of Work or other contract between the parties:

"Personal Information" are the categories of personal data defined by the CCPA that can identify, relate to, describe, be associated with, or be reasonably linked directly or indirectly to a particular consumer or household, including, without limitation: household purchase data, family information, financial information, geolocation, biometric data and sleep information."

Further, the following definitions, as set forth by the GDPR, shall apply to this Policy, the Agreement or relevant Scope of Work or other contract between the parties:

1. "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
2. "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately.
3. "Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
4. "Controller" means the natural or legal person, public authority, AOR or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where

the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

5. "Processor" means a natural or legal person, public authority, AOR or any other body which processes personal data on behalf of the controller.

6. "Subprocessor" means any third-party data processor engaged by and contracted with a Processor for purposes of processing Data.

7. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

AOR and Client may address the following in a Scope of Work or other writing:

- the subject matter and duration of the processing;
- the nature and purpose of the processing (the reason information will be collected);
- the type of personal data and categories of data subject; and
- the obligations and rights of the Controller (the Client shall serve as the Controller).

GENERAL AOR POLICIES REGARDING PRIVACY AND DATA SECURITY

AOR will make commercially reasonable efforts to comply with the predominant privacy and data security laws and regulations, including the CCPA, applicable solely to the services AOR will provide to Client.

AOR will comply with Client's data security or privacy policies only provided that Client's policies are substantially similar to AOR's policy regarding the provided AOR services.

AOR and Client will work together to protect all Data by adherence to the following general principles:

- Client will only provide AOR with Data or information necessary for AOR's performance of the work set forth in a Scope of Work.
- Client will provide notice to the senior AOR executive handling the Client's account prior to transmitting any Data or information, so that the parties can establish required security notices or information process filters in advance of transmission. In the case of Personal Information, AOR may require advance written consent prior to receipt.
- AOR will designate the appropriate individuals to receive Data from Client or any third parties on behalf of Client.

Sensitive Personal Data: When the Scope of Work entails AOR handling of Sensitive Personal Data, at the time a specific Scope of Work is contemplated, Client and AOR will jointly establish the data security risk, control measures and any enhanced responsibilities of each party with respect to the Sensitive Personal Data. Sensitive Personal Data means data that consists of either Personal Data, Client customer information, customer financial information, or any additional information designated in writing by Client

as highly sensitive. In the event additional or more stringent data security requirements are required to handle Sensitive Personal Data, those requirements will be separately outlined in the Scope of Work project specifications. Those more stringent data security requirements will apply only to the identified Sensitive Personal Data, and to any Scope of Work project that involves the Sensitive Personal Data.

In the event AOR is required to institute additional, more costly or more stringent measures to use, handle or store the Data, and incurs additional costs related to such measures, AOR will advise Client in advance of incurring these expenses, and Client will be responsible for such expenses.

In the event AOR is required to institute additional or more stringent security measures to use, handle, or store the Data, such additional or enhanced measures may cause delays in completion or implementation of work or services. AOR is not responsible for such delays, or any increased costs or expenses incurred by Client related to such delays.

Personal Data: When and if the Scope of Work entails AOR handling of Personal Data , Client and AOR will jointly establish the Data security risk, control measures and any enhanced responsibilities of each party with respect to the Personal Data. Personal Data means any data that could potentially identify a specific individual or can be used to distinguish one person from another and can be used for de-anonymizing anonymous data (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).

Personal Information Handling Procedures

When the Scope of Work entails AOR handling of Personal Information, at the time a specific Scope of Work is contemplated, Client and AOR will jointly establish the data security risk, control measures and any enhanced responsibilities of each party with respect to the Personal Information. In the event additional or more stringent data security requirements are required to handle Personal Information, those requirements will be separately outlined in the Scope of Work project specifications. Those more stringent data security requirements will apply only to the identified Personal Information, and to any Scope of Work project that involves the Personal Information.

In the event AOR is required to institute additional, more costly or more stringent measures to use, handle or store the Data, and incurs additional costs related to such measures, AOR will advise Client in advance of incurring these expenses, and Client will be responsible for such expenses.

In the event AOR is required to institute additional or more stringent security measures to use, handle, or store the Data, such additional or enhanced measures may cause delays in completion or implementation of work or services. AOR is not responsible for such delays, or any increased costs or expenses incurred by Client related to such delays.

RESPONSIBILITIES OF CLIENT

Client will maintain commercially reasonable privacy and data security processes, and will employ measures to avoid misuse or wrongful transfer of Data to AOR.

Client will not provide AOR, or induce any third party to provide AOR, with any Data or information that is improperly sourced, or obtained by any mean or method that does not comply with applicable privacy or data security laws, regulations, rules, or industry codes or guidelines, including but not limited to CCPA or GDPR.

Client will provide AOR only with Data or information necessary for AOR's performance of work set forth in a Scope of Work.

Client may be subject to additional privacy or data security laws and regulations, rules, or industry codes and guidelines, including but not limited to CCPA or GDPR, unrelated to the specific work or services provided by AOR. In such case, Client is solely responsible for compliance with those laws or regulations.

Client will provide AOR with sufficient advance notice of any necessary additional, or more stringent, measures required for AOR to use, handle or store the Data. Client will provide such notice to provide AOR a reasonable amount of time to evaluate and, as necessary, prepare for, the additional or more stringent measures required.

Client is responsible for obtaining any required consents or acknowledgements from AOR prior to transmitting or sharing of any Data, and will request and obtain such consents or acknowledgments in a timely manner to as to allow AOR to conduct a reasonable review of the request.

Client is responsible for any increased costs associated with instituting additional, more costly or more stringent measures required for AOR to use, handle or store the Data. Client will pay such costs promptly upon notification by AOR of them. In some cases where reasonable and appropriate, AOR may request Client to advance such costs.

Client will have an up-to-date privacy policy on its website(s) that: (i) complies with all applicable country and local privacy and data protection laws, that are applicable only to Client's business and services; (ii) accurately discloses all applicable data collection, use and disclosure practices, including the use of cookies, pixels, beacons, locally stored objects or other similar technologies for purposes of targeting individual end users with advertisements (iii) discloses the use of one or more third parties for ad serving activities, if applicable; (iv) contains a statement that its site or app permits limited data collection, based only on data that does not personally identify consumers, for interest-based advertising; (v) contains a description of the non-personally identifiable types of data collected for such advertising; and (vi) contains an explanation of the purposes for which data is collected by, or transferred to, third parties, if applicable.

Client will make commercially reasonable efforts to conspicuously post a link to its privacy policy on its website(s), mobile app(s) and in relevant app store(s). Such privacy policies must provide end users with a conspicuous link to a functional opt-out page.

RESPONSIBILITIES OF AOR

AOR will act on the written instructions of the Client (unless required by law to act without such instructions or such instructions are contrary to relevant laws or regulations);

AOR will ensure that people in its employment with access to the Data or otherwise processing the Data are subject to a confidentiality agreement or policy;

AOR will provide reasonable assistance to the Client in providing subject access and allowing data owners of Personal Information to exercise their rights under the CCPA or GDPR;

AOR will keep records of its activities regarding the Data in accordance with the CCPA or GDPR;

AOR will delete, destroy, or return all Personal Data or Personal Information to the Client as requested at the end of the contract; and

AOR will provide reasonable cooperation in audits and inspections, and provide the Client with whatever information in its possession the Client needs to ensure that both parties are meeting their CCPA or GDPR obligations, and tell the Client immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

AOR must take appropriate measures to ensure the security of processing and notification of personal Data Breaches and data protection impact assessments;

AOR must only engage a Subprocessor with the prior consent of the Client and a written contract;

AOR must assist the Client in providing subject access and allowing data subjects to exercise their rights under the GDPR;

AOR will employ a data protection officer if required in accordance with the GDPR; and

AOR will appoint (in writing) a representative within the European Union if required in accordance with the GDPR.

RESPONSIBILITIES OF THIRD PARTIES

In the event of the engagement by Client of any third party suppliers or services to obtain or collect, curate, store, or otherwise use relevant Data, AOR will not be responsible for guaranteeing the performance of third party suppliers or indemnifying Client for a Data privacy or security breach arising out of the conduct of third party suppliers or services. Indemnification obligations related to services provided by third party suppliers should be the responsibility of the third party supplier and will be incorporated in the agreement between the third party supplier and Client. Client will procure a written agreement with any third party supplier or service it engages to reflect the indemnification responsibilities of that third party.

Where a third party vendor will be charged with obtaining or collecting, curating, storage of, or other use of Data, AOR and Client may collaborate to review the proposed agreement and Scope of Work documents with the third party to ensure that they include the necessary and specific Data privacy and security requirements, however Client will not assume responsibility for any negligence or noncompliance of the third party where it contracts directly with that third party.

Where a third party is directly subcontracted by the AOR (a Subcontractor), such third party indemnification obligations of the Subcontractor will be incorporated into the agreement between AOR and the Subcontractor, with the Client a beneficiary thereof. All subcontractors will be expected to comply with the same (or substantially similar) Data security, privacy, and confidentiality terms that are applicable to the AOR.

COMPLIANCE VERIFICATION

AOR will promptly and reasonably respond to any requests of Client to verify AOR's compliance with any agreed Data privacy and security measures. The scope of verification required, including the length or depth of any compliance review, will be determined jointly by the parties, based upon the type and amount of Data collected by AOR, and any agreed measures and protocol for maintaining Data privacy and security. The review will be no broader than necessary to determine AOR's compliance.

LIABILITY LIMITATION

Client will remain directly liable for compliance with all aspects of the GDPR and CCPA, and for demonstrating that compliance, including all compliance by AOR and any of its subcontractors, unless Client can prove that it was not in any way responsible for the event giving rise to the damage. Otherwise, Client will be fully liable for any damages, losses, claims and liabilities caused by non-compliant handling of Data, regardless of its use of AOR to assist in management or processing of Data.

INDEMNIFICATION

Client will indemnify and hold AOR harmless from Client's negligence or intentional failure to comply with relevant privacy or data security laws and regulations, rules, or industry codes and guidelines, including the CCPA or GDPR, relevant to any Data in possession or control of AOR related to a Scope of Work between the parties.

Client will indemnify and hold AOR and its Subcontractors harmless for any claims, liabilities, losses, or damages caused by non-compliant processing or breach of duties by AOR or its Subcontractors.

Client will also indemnify and hold AOR and its Subcontractors harmless for any non-compliance with all aspects of relevant privacy or data security laws and regulations, rules, or industry codes and

guidelines, including the CCPA or GDPR, and for demonstrating that compliance to regulators as required, including all compliance by AOR and any of its Subcontractors.

AOR will indemnify and hold Client harmless solely where: 1) AOR has failed to comply with CCPA or GDPR provisions for which it has specifically assumed responsibility in writing in a Proposal or Scope of Work, or ii) AOR has acted against the lawful written instructions of Client.
AOR will indemnify and hold Client harmless solely from its gross negligence or intentional act in selection of or failure to adequately supervise a Subcontractor (where AOR selected and contracted with such Subcontractor), which gross negligence or intentional act creates a liability of Client for failure to comply with relevant privacy or data security laws and regulations, rules, or industry codes and guidelines, including the CCPA or GDPR, relevant to Data in possession or control of the Subcontractor related to a Scope of Work between the parties.

Each party's liability to the other party to remediate or for any Data privacy or security breach, or any failure to comply with relevant privacy or data security laws and regulations, rules, or industry codes and guidelines, including the CCPA or GDPR, shall not exceed the total fees paid pursuant to the relevant Agreement, Scope of Work, or other written agreement(s) between the parties.