Data Processing Addendum

This Data Processing Addendum ("Addendum" or "DPA"), effective as of the effective date of the Master Client Agreement (the "Principal Agreement" for the purposes of this DPA) forms part of the written or electronic agreement between Client and Integrated Research (as defined below, "IR"), acting on its own behalf and as agent for each of its Affiliates, including any work orders, purchase orders, addenda, or exhibits thereto. The Integrated Research entity that is a party to the Principal Agreement is a party to this Addendum.

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. This DPA shall become effective upon the commencement of the Principal Agreement, be coterminous with the Principal Agreement, and shall control over any contrary terms in any Exhibit or other ancillary agreement or terms to the Principal Agreement.

In consideration of the mutual obligations set out herein, the parties hereby agree as follows:

1. Definitions

"**Affiliate**" means any entity that is controlled by, or is under common control with the subject entity, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract, or otherwise.

"**Anonymized Data**" means anonymized information derived from User Data so long as (i) no personally identifiable information may be derived from such Anonymized Data, and (ii) such Anonymized Data cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.

"**CCPA**" means the California Consumer Privacy Act of 2018, as amended from time to time, and the regulations promulgated thereunder.

"**Client Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Client pursuant to or in connection with the Principal Agreement.

"**Contracted Processor**" means IR or a Subprocessor.

"**Data Protection Law(s)**" means the applicable data protection or privacy laws of any country.

"**Data Subject**" means a natural person whose Personal Data is processed by IR and to whom at least one Data Protection Law applies.

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

"**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 by the GDPR and laws implementing or supplementing the GDPR.

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

"**Integrated Research**" or "**IR**" means the Integrated Research entity which is a party to this Addendum, as specified in the introductory paragraph above, being one of: Integrated Research Limited, a company incorporated in New South Wales Australia; Integrated Research, Inc., a company incorporated in Colorado United States; Integrated Research UK Limited, a company incorporated in the United Kingdom; Integrated Research Pte. Limited, a company incorporated in Singapore; and Integrated Research Germany GmbH, a company incorporated in Germany.

"Personal Data" means any information relating to an identifiable natural person, an identifiable natural person is one who can be identified, directly or indirectly, in particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Personal Data Breach**” means any breach of the security and/or confidentiality requirements of this Addendum involving or leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data processed by IR on behalf of Client, or any indication of such breach having taken place or being about to take place.

"**Restricted Transfer**" means: (a) a transfer of Client Personal Data from Client to a Contracted Processor; or (b) an onward transfer of Client Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor. In each case, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses. A Restricted Transfer does not include transfers of Personal Data authorised by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme which is approved as ensuring an adequate level of protection or any transfer which falls within a permitted derogation.

"**Services**" means the services to be supplied to or carried out by or on behalf of IR for Client pursuant to the Principal Agreement.

"**Standard Contractual Clauses**" or “**SCCs**” has the meaning set forth in **Exhibit A**.

"**Subprocessor**" means any corporation, entity or other legal person (including any third party and any IR Affiliate), appointed by or on behalf of IR or any IR Affiliate to Process Personal Data on behalf of Client in connection with the Principal Agreement.

The terms, "Controller", "Member State", "Processing/Processor" and shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority; Controller

2.1. IR warrants and represents that, before any IR Affiliate Processes any Client Personal Data on behalf of Client, such IR Affiliate will have agreed to terms at least as protective of Client Personal Data as provided in this Addendum.

2.2. For the purposes of the GDPR and substantially similar Data Protection Laws, IR is an independent Controller with respect to IR’s processing of Personal Data collected through its website, services analytics, and any other lawful data processing not performed on behalf of Client or in which IR performs as a Controller. The subject matter, nature, purpose, and duration of processing, as well as the types of Personal Data collected and categories of Data Subjects, are as described in Exhibit A or the Principal Agreement. IR will process such data as further set forth herein, including: billing and account management, analytics for internal improvements of the Services, securing its systems and combating fraud, and as further set forth under the Principal Agreement. Apart from this DPA, IR handles information collected through IR’s website or from individual users as set forth in the IR Privacy Policy.

3. Processing of Client Personal Data

3.1. IR shall:

a) comply with all applicable Data Protection Laws in the Processing of Client Personal Data; and

b) not Process Client Personal Data other than on Client’s documented instructions in the Principal Agreement and this DPA, and as reasonably necessary for IR to perform its obligations under the Principal Agreement, unless Processing is required by Data Protection Laws.

3.2. Notwithstanding anything to the contrary in the Principal Agreement, nothing herein shall be deemed to prohibit IR from aggregating, analysing, using, disclosing, and otherwise using Anonymized Data for any lawful purpose under applicable law so long as (i) no Personal Data may be derived from such Anonymized Data, and (ii) such Anonymized Data cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.

3.3. Client:

a) instructs IR (and authorises IR to instruct each Subprocessor) to:

i) Process Client Personal Data;

ii) transfer IR Personal Data to any IR Affiliate country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement.

b) warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in Section 3.3.a) on behalf of each IR Affiliate processing Client Personal Data.

3.4. The Exhibits to this Addendum set out certain information regarding the Contracted Processors' Processing of Client Personal Data as required by applicable Data Protection Laws. IR may make reasonable amendments to an applicable Exhibit by written notice to Client from time to time as IR reasonably considers necessary to meet the requirements of new or amended Data Protection Laws.

3.5. Client represents and warrants that it has the legal right to make the Personal Data available to IR for the Services and, where prescribed by Data Protection Laws, has secured consent and provided notice to Data Subjects. Client will upon IR's request make available reasonable documentation satisfactory to IR to demonstrate its compliance with this Section. Client will only provide instructions to IR that are lawful and will comply with and perform its obligations under Data Protection Laws, including with regard to data subject rights, data security and confidentiality, and ensuring an appropriate legal basis for processing of Personal Data.

4. IR Personnel

IR shall take reasonable steps to ensure:

a) any employee, agent or contractor of any Contracted Processor who may have access to the Client Personal Data is bound by confidentiality and privacy obligations no less protective of Personal Data than this Addendum;

b) that access is strictly limited to those individuals who need to know or access the relevant Client Personal Data for the purposes of performing the Principal Agreement;

c) compliance with Data Protection Laws in the context of that individual's duties to the Contracted Processor; and

d) that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the associated risk to the rights and freedoms of natural persons, IR shall, in relation to the Client Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including measures as required under Data Protection Laws.

6. Subprocessing

6.1. To the extent required under applicable Data Protection Laws, Client authorises IR to appoint (and permit each Subprocessor appointed in accordance with this Section 6 to appoint) Subprocessors in accordance with this Section 6 and any restrictions in the Principal Agreement.

6.2. IR may continue to use those Subprocessors listed on its Subprocessor List, available at: www.ir.com/legal so long as the requirements set out in Section 6.4 are met.

6.3. IR shall give Client prior written notice, through update of the Subprocessor List or communication through the IR Services, of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within ten (10) business days of receipt of that notice, Client notifies IR in writing of its reasonable objections to the proposed appointment:

a) IR may, in its sole discretion, attempt to resolve Client's objection, including providing the Services without use of the new Subprocessor. If IR provides Client written notice that it will not pursue an alternative, or such an alternative cannot be made available by IR to Client within 90 days of Client providing notice of its objection, then in either case, IR will:

i) work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor or addresses such objections; or

ii) where such a change cannot be made, notwithstanding anything in the Principal Agreement, Client may immediately terminate the applicable order to the extent that it relates to the Services which require the use of the proposed Subprocessor.

6.4. With respect to each Subprocessor, IR shall ensure that IR, or the relevant intermediate Subprocessor, as applicable, and the Subprocessor have a written contract in place that includes terms substantially similar to the terms set out in this Addendum with regard to the protection of Client Personal Data.

7. Data Subject Rights

7.1. Taking into account the nature of the Processing, IR shall implement appropriate technical and organisational measures to assist IR in responding to requests to exercise Data Subject rights under the Data Protection Laws.

7.2. IR shall:

a) promptly notify Client if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data; and

b) ensure that the Contracted Processor does not respond to the Data Subject request except on the documented instructions of Client, the relevant Client Affiliate, or as required by Data Protection Laws to which the Contracted Processor is subject, in which case IR shall to the extent permitted by Data Protection Laws inform Client of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1. IR shall notify Client without undue delay upon IR or any Subprocessor becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. With respect to Personal Data Breaches in which IR is a processor, IR will provide information sufficient to enable the Client as Controller to perform a thorough investigation, formulate a correct response, and to take suitable further steps. Such notification shall at a minimum:

a) describe the nature of the Personal Data Breach, the categories and number of Data Subjects concerned, and the categories and number of Personal Data records concerned;

b) communicate the name and contact details of IR's data protection officer or other relevant contact from whom more information may be obtained;

c) describe the likely consequences of the Personal Data Breach; and

d) describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2. IR shall cooperate with Client and take such reasonable commercial steps, taking into account Client’s reasonable requests to assist in the investigation, mitigation and remediation of each such Personal Data Breach, to the extent such Personal Data Breach is caused by an act or omission of IR, a Subprocessor, or an IR Affiliate.

9. Data Protection Impact Assessment and Prior Consultation

IR will provide Client with reasonable cooperation and assistance needed with any Client data protection impact assessments (or similar requirement under Data Protection Laws), and prior consultations with supervising governmental authorities or other applicable data privacy authorities, which Client reasonably considers to be required for Client to fulfil its obligations under any applicable Data Protection Laws. If IR believes or becomes aware that its processing of the Client Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, or IR no longer believes it can abide by the terms of this Addendum or Data Protection Laws, it will promptly inform Client and provide Client with all such reasonable and timely assistance as Client may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

10. Deletion or return of Client Personal Data

Upon termination or expiration of the Principal Agreement and unless explicitly set forth to the contrary in the Principal Agreement, IR will (upon Client's election and request) destroy or return to Client all Client Personal Data (including all copies of the Data) in its possession or control. This requirement will not apply to the extent that IR is required by any Applicable Law to retain some or all of the Personal Data, in which event IR will isolate and protect the Client Personal Data from any further processing except to the extent required by such law. The foregoing requirement will not apply to copies automatically retained by IR's backup and security systems (i.e. system logs) which may not be deleted without undue expense.

11. Audit rights

11.1. Subject to Section 11.2, during the term of the Principal Agreement, IR shall make available to Client upon reasonable request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Client or a mutually agreed third-party auditor in relation to the Processing of the Client Personal Data by the Contracted Processors. Client shall be responsible for the costs associated with such audit.

11.2. Information and audit rights of Client only arise under Section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

12. Restricted Transfers

12.1. Except as authorized by this Addendum, IR shall not disclose Personal Data received by or on behalf of Client to a third party or transfer it to another country without the Client's authorization or as prescribed by Data Protection Laws. Except as otherwise provided herein, IR shall immediately notify the Client of any planned permanent or temporary transfers of Personal Data to a country outside of the country in which Client provides or makes available Client Personal Data.

12.2. To the extent that IR or the Client are relying on a specific statutory mechanism for compliant international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, IR and Client agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer under Data Protection Laws.

12.3. IR and Client will not execute any country-specific contractual means of accomplishing a Restricted Transfer in accordance with Data Protection Laws unless its effect is to allow the relevant Restricted Transfer to take place without breach of such Data Protection Law.

12.4. For Restricted Transfers from the EU, EEA, UK, or Switzerland, Client (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") will enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Client to that Contracted Processor as set forth on **Exhibit A**.

12.5. For Restricted Transfers from Singapore, IR and Client agree to the additional terms set forth on **Exhibit B**.

12.6. For Personal Data originating in India, IR and Client agree to the additional terms set forth on **Exhibit C**.

12.7. When IR acts as a Service Provider or joint Business under the CCPA, **Exhibit D** will apply.

13. Limitation of Liability

13.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, and all data processing agreements between the parties whether in contract, tort, or under any other theory of liability, shall not exceed the fees paid by Client to IR in the 12 months preceding the transaction or act giving rise to the claim. The foregoing limit is cumulative for all claims against that party and all of its Affiliates under the Principal Agreement and all data processing agreements between the parties.

14. General Terms

14.1. **Governing law and jurisdiction**

Without prejudice to clauses 18 (Choice of Forum and Jurisdiction) and 17 (Governing Law) of the Standard Contractual Clauses:

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

b) this Addendum 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 such purpose in the Principal Agreement.

14.2. **Order of precedence**

With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum 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 Addendum, the provisions of this Addendum shall prevail.

14.3. **Survival.**

Sections 2.2, 3.2, 6, 10, and 13 shall survive the termination of this DPA.

14.4. **Severance**

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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.

EXHIBIT A

Transfers of Personal Data from the EU, EEA, UK, or Switzerland

Transfers of Personal Data from the European Union, European Economic Area, Switzerland, or the United Kingdom of Great Britain and Northern Ireland ("UK") to third countries are subject to the Standard Contractual Clauses, Module Two (Controller to Processor). The SCCs are hereby incorporated into the Addendum and the parties' acceptance of this Addendum shall constitute the parties' acceptance and signing of the Standard Contractual Clauses. If the terms of the Addendum conflict with the SCCs, the terms of the SCCs will prevail.

As used herein, "Standard Contractual Clauses" or "SCCs" means (i) the standard contractual clauses for international transfers published by the European Commission on June 4, 2021 governing the transfer of European Area Personal Data to Third Countries as adopted by the European Commission and the Swiss Federal Data Protection and Information Commissioner ("Swiss FDPIC") relating to data transfers to Third Countries (collectively "EU SCCs"); (ii) the international data transfer addendum ("UK Transfer Addendum") adopted by the UK Information Commissioner's Office ("UK ICO") for data transfers from the UK to Third Countries; or (iii) any similar such clauses by a data protection regulator relating to data transfers to Third Countries; or (iv) any successor clauses to (i) – (iii).

The Standard Contractual Clauses set forth below shall come into effect under Section 12.4 of the DPA on the later of:

a) the data exporter becoming a party to them;

b) the data importer becoming a party to them; and

c) commencement of the relevant Restricted Transfer.

The Standard Contractual Clauses will be deemed incorporated into this Addendum and shall apply as completed below:

A. In Clause 7, the "Docking Clause (Optional)", will be deemed incorporated.

B. In Clause 9, Option 2 is selected, and the time period for prior notice of addition or replacement of Subprocessors will be as set forth in the Addendum.

C. In Clause 11, the optional language will not apply.

D. In Clause 13, the competent supervisory authority shall be the Bavarian Data Protection Commission where the EU SCCs apply, the FDPIC where the Swiss DPA applies and the UK Information Commissioner where the UK Transfer Addendum applies.

E. In Clause 17, Option 2 is selected, and the Standard Contractual Clauses will be governed by the laws of Germany where the EU SCCs apply, the law of Switzerland where the Swiss DPA applies and the law of England and Wales where the UK Transfer Addendum applies.

F. In Clause 18(b), disputes will be resolved before the courts of Ireland where the EU SCCs apply, the courts of Switzerland where the Swiss DPA applies and the courts of England and Wales where the UK Transfer Addendum applies.

G. Annexes I and II of the SCCs are as set forth below; and Annex III is as set forth in the Subprocessor List.

H. For the purposes of the UK Transfer Addendum, the Standard Contractual Clauses will be interpreted in accordance with Part 2 of the UK Transfer Addendum; Sections 9 – 11 of the UK Transfer Addendum will override Clause 5 of the EU SCCs and both the "Importer" and "Exporter" shall be able to end the UK Transfer Addendum as set out in Section 19 of the UK Transfer Addendum.

ANNEX 1

DETAILS OF PROCESSING PERSONAL DATA

A. LIST OF PARTIES, DETAILS OF PROCESSING

MODULE TWO: Transfer controller to processor

Data exporter(s): Client

Role (controller/processor): Controller

Data importer(s): Integrated Research

Role (controller/processor): Processor

Subject matter and duration of the Processing of Personal Data:

The personal data transferred will be subject to the following basic processing activities:

IR will process Personal Data as necessary to perform the Services for Client pursuant to the Principal Agreement.

The Duration of the processing of Personal Data will be the duration of the Services to be provided under the Principal Agreement.

Categories of Personal Data to be Processed:

The Personal Data to be processed may include the following categories of data subjects:

- Employees of Client, including temporary or contract workers
- Clients and business partners of Client

Type of Personal Data to be Processed (check all that apply):

☒ Client Address
☒ Client Company Information
☒ Email
☒ First Name
☒ Last Name
☒ Hostname
☒ MAC address
☒ Phone number
☒ Server IP address
☒ Account name
☒ Username and/or password

Legal Basis for Processing:

The Processing is necessary for the performance of the Principal Agreement. In addition, Controller has a legitimate interest in IR's services to provide enterprise IT performance management software and services.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred: ***Controller's employees and contractors***

………………………...

Categories of personal data transferred: ***See Above***

………………………...

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, *access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:* **None**

………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). ***Daily or as required to provide the software and services.***

…………………………

Nature of the processing: ***Processor provides enterprise IT performance management software and services.***

…………………………

Purpose(s) of the data transfer and further processing: ***For Processor to fulfill its obligations under the Principal Agreement.***

………………………..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: ***The duration of the Principal Agreement***.

……………………..

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: ***Hosting and cloud providers as required for Processor to deliver the software and services for the duration of the Principal Agreement.***

……………………..

Exhibit B

Additional Terms for Personal Data Originating in Singapore

1. **Legitimate Interest**. Personal Data originating in Singapore and processed by IR on behalf of Client is processed pursuant to Client's legitimate interest in improving communications between Client Data Subjects and employees through the Services. IR shall not market to any employees or users of Client using Personal Data collected solely through the Services during the course and for the purposes of the individual's employment, business, or profession.
2. **Assessment**. IR has conducted an assessment under Section 15 of the Singapore Personal Data Protection Regulations 2021("PDPA") before collecting, using, or disclosing the Client Personal Data to determine the applicability of the legitimate interests exception, including identifying any adverse effect that the proposed collection, use, or disclosure may have on the individual. A copy of the assessment conducted throughout the period that IR collects, uses, or discloses the Client Personal Data under the legitimate interests exception is available upon request.

3. **Transfer Agreement Requirements**. IR provides a standard of protection for the Personal Data transferred via the Services ("Transferred Data") that is at least comparable to the PDPA's protection requirements.
   - Transferred Data will be transferred to the countries mentioned in the Principal Agreement and to the countries in which authorized Subprocessors host their services.
   - The purpose of collection, use, and disclosure for the Transferred Data is set forth in **Exhibit A**.
   - IR agrees to keep the Transferred Data secure, accurate, and complete to a reasonable standard.
   - IR's retention limits for the Transferred Data are as set forth in Section 10 of the Addendum.
   - IR's policies on Personal Data protection are as set forth in its Privacy Policy, available at: https://www.ir.com/legal/privacy-policy. Individuals' rights to access and correct Personal Data held by IR are as set forth therein.

Exhibit C

Additional Terms for Personal Data Originating in India

1. Personal Data Breaches. The term "Personal Data Breach" when used with respect to Personal Data originating in India and processed by IR by or on behalf of Client, shall also include:

(a) a complaint or a request with respect to the exercise of a data subject's rights under Indian Data Protection Laws; and

(b) where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate Data Protection Laws to which Client or IR are subject.

2. Incident Response. IR shall at all times have in place written procedures which enable it to promptly respond to the Client about a Personal Data Breach. Where a Personal Data Breach is reasonably likely to require a data breach notification by IR under the Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, IR shall implement its written procedures in such a way that it is in a position to notify the Client no later than 24 hours of having become aware of such an incident.

Exhibit D

Additional Terms for Personal Information of California Consumers

This Exhibit applies to the extent that IR is acting as a Service Provider processing Client's California Consumer Personal Information.

1. Definitions. In this Exhibit D only, "Regulations" means applicable regulations promulgated by the California Privacy Protection Agency, as amended. The terms "Business," "Business Purpose," "Collects," "Consumer," "Person," "Personal Information," "Sell," "Service Provider," and "Share," shall have the meaning set forth in the CCPA.

2. Business and Service Provider. The Principal Agreement documents the Business Purpose for which IR is processing the Personal Information. Client discloses Personal Information to IR only for such limited and specified Business Purpose. The parties agree that Client is a Business and IR is a Service Provider, or Business only if set forth in the Principal Agreement.

3. Processing Restrictions. In respect of the Personal Information Processed in the course of fulfilling the Business Purpose to Client, IR:

3.1 shall not sell or share Personal Information it collects pursuant to the Principal Agreement;

3.2 shall not retain, use or disclose the Personal Information it collects pursuant to the Principal Agreement for any purpose other than the Business Purpose, or as otherwise permitted by the CCPA and the Regulations;

3.3 shall not retain, use or disclose the Personal Information it collects pursuant to the Principal Agreement for any commercial purpose other than the Business Purpose, unless expressly permitted by the CCPA or the Regulations;

3.4 shall not retain, use, or disclose the Personal Information it collects pursuant to the Principal Agreement outside the direct business relationship between Client and IR, unless expressly permitted by the CCPA or the Regulations. Specifically, IR shall not combine or update Personal Information with Personal Information it has received from another source or collected from its own interaction with the Consumer, unless expressly permitted by the CCPA or the Regulations;

3.5 shall comply with all applicable sections of the CCPA and the Regulations, including - with respect to the Personal Information that it collects pursuant to the Agreement - provision of the same level of privacy protection as required of Businesses by the CCPA and the Regulations; and

3.6 may, subject to the Principal Agreement, engage another Person to assist IR to fulfil the Business Purpose; provided, however, that IR must enter into a written agreement with a Person that complies with this Exhibit, the CCPA, and the Regulations, including Section 7051(a).

4. Audit. Client has the right, upon advance written notice, to take reasonable and appropriate steps to ensure that IR uses the Personal Information in a manner consistent with the Business's obligations under the CCPA and the Regulations. If, after completing the assessment described herein, Client determines that IR may be in violation of its obligations in this Addendum, the CCPA or the Regulations, then upon advance written notice, Client has the right to take reasonable and appropriate steps to stop and remediate IR's unauthorized use of Personal Information.

5. Conflict. Any conflict between the terms of this Exhibit, the Addendum, or the Principal Agreement related to the processing of Client Personal Data are resolved in the following order of priority: (1) the CCPA, (2) this Exhibit, (3) the Addendum, and then (4) the Principal Agreement.