DATA PROCESSING ADDENDUM
SOFTWARE SERVICES

This Data Processing Addendum ("**DPA**") is entered into by TypeA Holdings Ltd. (“**Company**”) and the counterparty using TypeA Software Services (“**Partner**”) both parties shall be referred to as the “**Parties**” and each, a “**Party**”. This DPA forms an integral part of the agreement executed between the Parties (“**Agreement**”) and governs the Software Services. Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

This DPA sets forth the parties’ responsibilities and obligations regarding the Processing of Personal Data (as such terms are defined below) during the term of the Agreement.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data. In the event of a conflict between this DPA and the SCC (as defined below) the SCC will prevail solely with regards to international transfer of Personal Data.

Company retains the exclusive right to modify or update this DPA, at any time, without prior notice, and at Company's sole discretion. Partner agrees that by continuing to use the services afterCompany has updated this DPA or provided Partner with notice thereof, Partner will be bound by the updated DPA. If Partner does not accept any modification to this DPA, its only recourse is to cease using the services.

1. Definitions and Interpretation

1.1 In this DPA:

1.1.1 “**Affiliate**” means any person or entity directly or indirectly controlling, controlled by, or under common control with a Party. For the purpose of this definition, "control" (including, with correlative meanings, the terms "controlling", "controlled by" and "under common control with") means the power to manage or direct the affairs of the person or entity in question, whether by ownership of voting securities, by contract or otherwise.

1.1.2 “**Approved Jurisdiction**” means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.1.3 “**Data Protection Laws**” means, as applicable, any and all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data processed by Company solely on behalf of Partner, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**GDPR**”), Data Protection Act 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. of 2018 ("**CCPA**"), including as modified by the California Privacy Rights Act (“**CPRA**”) and any amendments or replacements to the foregoing.

1.1.4 “**Data Subject**” means a natural person to whom Personal Data relates.

1.1.5 “**Personal Data**” means any relating to an identified or identifiable natural person, and that is processed by Company on behalf of Partner in the context of the performance of the Agreement.

1.1.6 “**Security Incident**” means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data breach will comprise a Security Incident.

1.1.7 “**Special Categories of Data**” means personal data as defined under Article 9 of the GDPR.

1.1.8 “**Standard Contractual Clauses**” refers to the applicable module of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European

Parliament and of the Council from June 4th 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

1.1.9 "**Effective Date**" means the effective date of the Agreement.

1.1.10 The terms "**controller**", "**process(ing)**" and "**processor**" as used in this DPA have the meanings given to them in Data Protection Laws. Where applicable, controller shall be deemed as a "**Business**" and processor shall be deemed to be a "**Service Provider**", as these terms are defined in the CCPA.

1.1.11 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

2.1.1 Company processes Personal Data that is made available by Partner, or on behalf of Partner, in connection with the Agreement;

2.1.2 The Data Protection Laws apply to the processing of Personal Data.

2.1.3 CCPA Specifications are further detailed in Annex IV ("**CCPA Addendum**").

3. Roles and Restrictions on Processing

3.1 If Company has access to or otherwise processes Personal Data pursuant to the Agreement, then Company shall:

3.1.1 only process the Personal Data in accordance with Partner's documented instructions and on its behalf, and in accordance with the Agreement and this DPA and related Attachments, unless required otherwise under applicable laws. In such case, Company shall, to the extent legally permitted, promptly notify Partner of such legal obligation;

3.1.2 take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision have access to and process, Personal Data;

3.1.3 without undue delay, and in any case within the period of time required in Data Protection Laws, assist Partner as needed to cooperate with and respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information (including details of the services provided by Company) related to Company's processing of Personal Data;

3.1.4 notify Partner without undue delay, and no later than seventy-two (72) hours, after becoming aware of a Security Incident;

3.1.5 provide full, reasonable cooperation and assistance to Partner in:

3.1.5.1 upon receipt of: (a) requests from Data Subjects to exercise their rights under the Data Protection Laws in connection with Personal Data processed under this DPA, including (without limitation) the right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing, or the right not to be subject to an automated individual decision making, the right to opt-out where applicable; and/or (b) any requests or inquiries from supervisory authorities, customers, or others, to provide information related to Company's processing of Personal Data under this DPA; shall: (i) direct such requests to Partner without undue delay, and (ii) not respond or act upon such requests without prior written approval from Partner; and (iii) promptly, and in any case within the period of time required in Data Protection Laws, provide full, reasonable cooperation and assistance to Partner in responding to and exercising such requests, except that the foregoing shall not apply only and insofar as it conflicts with Data Protection Laws.

3.1.6 only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

3.1.7 as required under Data Protection Laws, maintain accurate written records of any and all the processing activities of any Personal Data carried out under the Agreement (including the categories of processing carried out and, where applicable, the transfers of Personal Data), and shall make such records available to the Partner and applicable supervisory authority on request; in the event the records and documentation provided are not sufficient for the purpose of demonstrating compliance, the Company shall make available, solely upon prior reasonable written notice and no more than once per calendar year, to a reputable auditor nominated by the Partner, information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the processing of the Personal Data ("Audit") in accordance with the terms and conditions hereunder. The auditor shall be subject to standard confidentiality obligations (including towards third parties). The Company may object to an auditor appointed by the Partner in the event the Company reasonably believes the auditor is not suitably qualified or is a competitor of the Company. The Partner shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, avoid causing any damage, injury or disruption to the Company's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit. Nothing in this DPA will require the Company to either disclose to Partner or its third-party auditor, or to allow Partner or its third-party auditor to access: (i) any data of any other customer; (ii) internal accounting or financial information; (iii) any trade secret; (iv) any information that, in the Company's reasonable opinion, could compromise the security of any systems or cause any breach of its obligations under applicable law or its security or privacy obligations to any third party; or (v) any information that Partner or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Partner's obligations under the Data Protection Laws;

3.1.8 not lease, sell or otherwise distribute Personal Data;

3.1.9 Partner shall be responsible to provide Company with any end-users' opt-out or consent signals to enable Compay to process the Personal Data in accordance with Data Protection Laws. With respect to Personal Data collected under this DPA via cookies/pixels/beacons or similar tracking technologies ("**Tracking Technologies**"), Compay will comply, where and when legally necessary, with end user's opt-out or consent signals transmitted via Partner's and/or its partners' consent mechanisms or otherwise; promptly notify Partner of any investigation, litigation, arbitrated matter or other dispute relating to the Company or the processing of Personal Data under the Agreement;

3.1.10 promptly notify Partner in writing and provide Partner an opportunity to intervene in any judicial or administrative process if Partner is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Personal Data to any person other than Partner;

3.1.11 upon termination of the Agreement, or upon Partner's written request at any time during the term of the Agreement, Company shall cease to process any Personal Data received from Partner, and within a reasonable period will at the request of Partner: (1) return the Personal Data; or (2) securely and completely destroy or erase all Personal Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws.

4. Sub-processing

4.1 The Company shall not subcontract its obligations under this DPA to another person or entity ("**Sub-processor(s)**"), in whole or in part, other than the Sub-processors detailed in Annex III, without providing the Partner with prior written notice, and shall inform Partner of any intended changes concerning the addition/replacement of other processors, no later than thirty (30) days prior to such intended change. Partner shall have the right to object to the appointment of any new Sub-processor within 7 days of having been notified of the Sub- processor's appointment by Company, in which event the Parties shall negotiate in good faith this objection. In the event the Parties, acting reasonably and in good faith, have not reached an amicable solution, then Partner may terminate the portion of the Agreement that requires the employment of said Sub-processor.

4.2 Company will execute a written agreement with such approved Sub-processor containing terms providing at least equivalent protection of Personal Data as provided under this DPA.

4.3 Company shall have a written security policy that provides guidance to its Sub-processors to ensure the security, confidentiality, integrity and availability of Personal Data and systems maintained or processed by Company.

4.4 Partner may require Company to provide Partner with full details of the proposed Sub-processor's involvement including but not limited to the identity of the Sub-processor, its data security record, the location of its processing facilities and a description of the access to Personal Data proposed.

4.5 Company shall be liable for the acts or omissions of Sub-processors to the same extent it is liable for its own actions or omissions under this DPA and Data Protection Laws.

5. Transfer of Personal Data

5.1 Where the GDPR is applicable, to the extent Company's Sub-processor processes Personal Data outside the EEA or Switzerland ("**EEA Transfer**") or an Approved Jurisdiction, such transfer shall be based on one of the appropriate safeguards in Article 46 of the GDPR.

5.2 If Company or its Sub-processors intend to rely on Standard Contractual Clauses, then if the Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this DPA, and Company without undue delay will begin complying with such Standard Contractual Clauses. Company will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or Sub-processor as the case may be.

5.3 The terms set forth in Part 1 of Schedule B shall apply to an EEA Transfer.

5.4 If the processing of Personal Data by Company includes a transfer (either directly or via an onward transfer) from the UK to other countries which has not been approved as providing an adequate level or protection to personal data by a decision of the UK Secretary of State, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Company for the lawful transfer of Personal Data (as defined in the UK GDPR) outside the UK ("**UK Transfer**"), then the terms set forth in Part 2 of Schedule B shall apply.

5.5 The terms set forth in Part 3 of Schedule B shall apply to an EEA Transfer and a UK Transfer.

6. Security Standards

6.1 Company shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; and all other unlawful forms of processing, as detailed in Annex II.

7. General

7.1 If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern solely with respect to matters relating to the processing of Personals Data. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

7.2 If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Data Protection Laws shall be deemed to be incorporated into this DPA, and each Party will promptly begin complying with such Data Protection Laws in respect of its respective processing activities.

Schedule B – Cross Border Transfers

Part 1: EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to transfer of Personal Data from the EEA to other countries that are not deemed as Adequate Countries.
2. This Schedule B sets out the Parties' agreed interpretation of their respective obligations under Module Two of the Standard Contractual Clauses.

3. The Parties agree that for the purpose of transfer of Personal Data between the Partner (Data Exporter) and the Company (Data Importer), the following shall apply:

    3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

    3.2. In Clause 9, option 1 shall apply. The Data Importer shall submit the request for specific authorization at least thirty (30) days prior to the engagement of the Sub-processor. Annex III shall be updated accordingly.

    3.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

    3.4. In Clause 13, the supervisory authority shall be Irish Data Protection Authority

    3.5. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland

    3.6. In Clause 18(b) the Parties choose the courts of Dublin, Ireland as their choice of forum and jurisdiction.

4. The Parties shall complete Annexes I–III below, which are incorporated in the Standard Contractual Clauses by reference.

Part 2: UK Transfers

1. This Part 2 is effective from the same date as the Standard Contractual Clauses.

2. This Part 2 is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and with respect to data transfers from controllers to processors and/or processors to processors.
3. Where this Part 2 uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

    a. “UK Data Protection Laws” shall mean all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

    b. “UK GDPR” shall mean the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

    c. “UK” shall mean the United Kingdom of Great Britain and Northern Ireland.
4. This Part 2 shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Part 2 shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.
7. In the event of a conflict or inconsistency between this Part 2 and the provisions of the Standard Contractual Clauses or other related agreements between the Parties, existing at the time the DPA is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.
8. This Part 2 incorporates the Standard Contractual Clauses which are deemed to be amended to the extent necessary so they operate:
   a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
   b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.
9. The amendments required by Section 8 above, include (without limitation):
   a. References to the "Clauses" means this Part 2 as it incorporates the Standard Contractual Clauses
   b. Clause 6 Description of the transfer(s) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."
   c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
   d. References to Regulation (EU) 2018/1725 are removed.
   e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"
   f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
   g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
   h. Clause 18 is replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
   i. The footnotes to the Clauses do not form part of this Part 2.
10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
11. The Parties may amend this Part 2 provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Standard Contractual Clauses and making changes to them in accordance with Section 8 above.
12. The Parties may give force to this Part 2 (incorporating the Standard Contractual Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Contractual Clauses.

PART 3 – Additional Safeguards

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
   a. Company shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from Partner to Company and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.
   b. Company will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act ("**FISA**");
   c. If Company becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

I. Company shall inform the relevant government authority that Company is a processor of the Personal Data and that Partner, the Controller, has not authorized Company to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon Partner in writing;

II. Partner will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under Company's control. Notwithstanding the above, Partner acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, Company has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (e)(II) shall not apply. In such event, Company shall notify Partner, as soon as possible, following the access by the government authority, and provide Partner with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, Company will inform Partner, at Partner's written request of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.

Annex I – Description of processing activities

A. Identification of Parties

"**Data Exporter**": Partner
"**Data Importer**": Company

B. Description of Transfer

Data Subjects

Partner's end-users.

Categories of Personal Data

IP addresses, IFV and IFA (e.g., IDFA/ AAID or any IDs), Privacy String, cookies data or unique identifiers, information about end-users' device.

Special Categories of Personal Data:

Not Applicable.

The frequency of the transfer

Continuous basis.

Nature of the processing

Collection, storage, organization, analysis, modification, retrieval, disclosure, communication and other uses in performance of the services as set out in the Agreement.

Purpose of the transfer and further processing

As defined in the Agreement.

Retention period

Personal Data will be retained for the term of the Agreement.

Annex II – SECURITY REQUIREMENTS

Each Party shall implement and maintain current and appropriate technical and organizational measures to protect Personal Data against accidental, unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, disclosure or access, as set forth below:

1. Provide third-party attestation of static or dynamic application security testing or penetration testing on all software or systems Processing Personal Data, remediate any identified high vulnerabilities, provide written remediation plans for medium and low vulnerabilities.
2. Maintain a level of security appropriate to the harm that may result from any unauthorized or unlawful Processing or accidental loss, destruction, damage, denial of service, alteration or disclosure, and appropriate to the nature of Personal Data;
3. Oblige its employees, agents or other persons to whom it provides access to Personal Data to keep it confidential; take reasonable steps to ensure the integrity of any employees who have access to Personal Data; provide annual training to staff and subcontractors on the security requirements contained herein;
4. Maintain measures designed to ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services;
5. Adhere password policies for standard and privileged accounts consistent with industry best practices;
6. Ensure that only those personnel who need to have access to Personal Data are granted access, such access is limited to the least amount required, and only granted for the purposes of performing the services and the obligations under this DPA;
7. Maintain a physical security program that is consistent with industry best practices;
8. Ensure that any storage media (whether magnetic, optical, non-volatile solid state, paper, or otherwise capable of retaining information) that captures Personal Data, if applicable, is securely erased or destroyed before repurposing or disposal;

Annex III – List of Sub-processors

Below is the list of the Data Importer's Sub-processors:

#	Name	Details	
1	**Amazon Web Services servers**	Address:	
		Contact details:	
		Description of processing:	
2	**GCP - BigQuery**	Address:	
		Contact details:	
		Description of processing:	
3	**Laminar Security**	Address:	
		Contact details:	
		Description of processing:	

Annex IV – CCPA Addendum.

This Annex IV CCPA Addemdum ("**Addendum**") is an integral part of the DPA which hereby adds specification applicable to the CCPA. All terms used but not defined in this Addendum shall have the meaning set forth in the DPA or as defined under the CCPA.

1. **Definitions:** The terms "**Business**", "**Business Purpose**", "**Consumer**", "**Contractor**", "**Cross-contextual Advertising**", "**Service Provider**", "**Sale**", "**Sell"** and "**Share**", shall have the same meaning as ascribed to them in the CCPA. When referencing Sections from this Addendum to the DPA a "**Data Subject**" shall also mean and refer to a "**Consumer**", and "**Personal Data**" shall include "**Personal Information**" under this DPA. "**Partner Data**" shall mean any Personal Information of California residents processed, shared, transmitted or used by the Company, on behalf of the Partner, for a Business Purpose identified by the Partner.

2. **Roles:** Partner is the Business and the Company is the Service Provider.

3. **Representation and Undertaking:** The Company shall process Partner Data as a Service Provider under the CCPA and shall not: **(i)** Sell or Share the Partner Data; (ii) retain, use or disclose the Partner Data for any purpose other than for a Business Purpose specified in the Agreement; or (iii) combine the Partner Data with other Personal Infromation that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents, expect as otherwise permitted by the CCPA.

4. **SPI:** if, and to the extent applicable, the Company shall assist Partner in respect of a Partner request to limit the use of its Sensitive Personal Information ("**SPI**").

5. **Data Process Assessment and Compliance with CCPA:** The Company shall provide information necessary to enable Partner to conduct and document any data protection assessments required by the CCPA. Notwithstanding the above, the Company is responsible for only the measures allocated to it. The Company agrees to notify the Partner if the Company reasonably determines that it can no longer meet its obligations under this Addendum or the CCPA.

6. **Consumer Request:** in addition to Section 4.1.5 and 4.1.7 of the DPA, the Company shall provide assistance and procures that its subcontractors will provide assistance, as Partner may reasonably request, where and to the extent applicable, in connection with any obligation by Partner to respond to Consumer's requests for exercising their rights under the CCPA.

7. **Sub-processors or Sub-contractors:** in addition to Section 5 of the DPA, the Company shall ensure confidentiality obligations are added to sub-processor agreement.

8. **Audit:** In addition to the Audit rights under Section 4.1.7 of the DPA, under US Data Protection Laws and subject to Partner's consent, the Company my alternately, in response to Partner's on premise audit request to initiate an independent auditing on its own, to verify its compliance with its obligations under this Addendum and the CCPA and provide the Partner with the results.

9. **Certification:** The Company certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from Selling or Sharing any Partner Data. The Company acknowledges and confirms that it does not receive any monetary goods, payments or discounts in exchange for processing the Partner Data.