CLARIO, INC.
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated into, forms a part of, and is in all respects subject to the terms of, the Master Services Agreement and Order(s) and Service Level Agreement between Customer and Clario, Inc. (the "**Agreement**"), collectively (the "**Parties**"), each entity (a "**Party**"). All capitalized terms that are not defined in this DPA will have the meanings assigned to those terms in the Agreement. In the event of any conflict or inconsistency among the documents within this Agreement, the order of precedence shall be: (1) the applicable Order, (2) this Agreement, and (3) any referenced schedule or linked document.

INTRODUCTION:

(A) Customer retained the Services of Clario under related Orders, which require Personal Data of the Customer's Data Subjects to be processed.

(B) In providing the Services, Clario will host, store, process, or have access to certain Personal Data relating to customers, suppliers, consultants, members of staff, or other individuals associated with Customer ("**Data Subjects**"), all as set out in the Data Processing Schedule. Personal Data of Data Subjects is to be processed by Clario solely for the purposes set out in the Data Processing Schedule ("**Customer Purpose**"), unless otherwise permitted under the terms of this DPA.

(C) Customer authorizes Clario to undertake the processing activities relating to Personal Data of Data Subjects in accordance with this Agreement, and Clario agrees to do so, all under the terms of this DPA.

THE PARTIES AGREE as follows:

1. INTERPRETATION
   - 1.1. In this Agreement, the following words and expressions shall, unless the context otherwise requires, have the meaning given to them below:
     - 1.1.1. "**Applicable Law**" means the Data Protection Laws, and any other laws in force in any country where Customer's Data may be processed under this DPA, or to which Clario or Customer may be subject.
     - 1.1.2. "**Customer's Data**" means Personal Data or Personal Information referred to in the Data Processing Schedule that Customer, or any person on its behalf, may transfer or make available to Clario for processing under this DPA (including any Personal Data or Personal Information that Customer, or any person on its behalf onto Clario's information systems or servers).
     - 1.1.3. "**Data Protection Laws**" means the California Consumer Privacy Act of 2018, as amended, and any other privacy and/or data protection state or federal law or regulation that applies to the Services or to the Parties.
     - 1.1.4. "**Data Processor**" or "**Processor**" means the entity which Processes Personal Data on behalf of the Customer; for purposes of this DPA, Clario is the Processor.
     - 1.1.5. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.
     - 1.1.6. "**Group**" refers to a Party and its Affiliates.
     - 1.1.7. "**Personal Data**" has the meaning given to such term or to similar terms such as "Personal Information" or "Personally Identifiable Information" in the Data Protection Laws.
     - 1.1.8. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("**Process**", "**Processes**" and "**Processed**" shall have the same meaning).

1.1.9. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.1.10. "**Subcontractor**" means any person who processes Customer's Data on behalf of Clario.

1.1.11. "**Term**" means the term of this Agreement in accordance with clause 10.1.

1.1.12. "**Third Party Partner**" means any entity engaged by Clario for the Processing of Personal Data.

2. DATA PROCESSING

2.1. The Parties agree that as between them and their Group members, for the purpose of the applicable Data Protection Laws, Customer is deemed the Business, and Clario shall be the Data Processor and the Service Provider (as such term is defined under the CCPA) in relation to any of Customer's Data processed by Clario (or its Subcontractors) under this Agreement or for the purpose of the Order(s).

2.2. Clario shall Process Customer's Data on behalf of Customer and strictly in accordance with the documented written instructions of Customer. For the avoidance of doubt, Customer authorizes Clario to Process Customers Data as set out in this Agreement (including the Data Processing Schedule).

2.3. In the event that Clario is required, by U.S. law or the applicable law of a U.S. state, or by an order of any U.S. federal or U.S. state court, or by a public authority in the U.S. or U.S. states under Applicable Law, to carry out any processing of Customer's Data not in accordance with the written instructions of Customer, Clario shall inform Customer of that legal requirement before carrying out the processing, unless that law prohibits such information on important grounds of public interest.

2.4. Clario shall not retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the Services specified in this Agreement with Customer, to retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the Data Protection Laws, for internal use by Clario to build or improve the quality of its services of which any Personal Data used would be anonymized and/or aggregated in such a manner that it no longer constitutes Personal Data under the applicable data protection laws, to detect data security incidents, or protect against fraudulent or illegal activity, to comply with federal, state, or local laws, to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities, to cooperate with law enforcement agencies concerning conduct or activity that Customer, Clario, or a third party reasonably and in good faith believes may violate federal, state, or local law, or to exercise or defend legal claims.

2.5. Clario shall not sell Personal Data. Clario shall further refrain from selling Personal Data on behalf of Customer when a Data Subject has opted out of the sale of his or her personal information with Customer.

2.6. Clario shall not collect, retain, use, or disclose Personal Data for a commercial purpose other than providing the Services specified in the Order(s) or this Agreement with Customer. For the avoidance of doubt, Clario shall not retain, use, or disclose Personal Data outside of the direct business relationship between Clario and Customer, unless otherwise permitted under the terms of this Agreement.

2.7. Clario shall comply with all Applicable Laws.

2.8. If, at any time, Clario receives notice that it is not in compliance with Applicable Law in regard to Customer's Data (such notice being received from any entity, including Customer, a Data Subject, or any other party), then Clario shall notify Customer immediately, and shall cure such non-compliance in accordance with Customer's written instructions.

3. CO-OPERATION

3.1. At Customer's request and cost, Clario shall assist Customer in ensuring compliance with Customer's obligations under the Data Protection Laws, in particular in relation to its obligations concerning: (a) Data Subject requests; (b) maintaining the security of Customer's Data processed

under this Agreement; (c) and notifications to regulatory authorities and communications to affected Data Subjects required in relation to events resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer's Data ("Data Breach").

3.2. Clario shall cooperate with Customer for all Data Subject requests. Clario shall delete Data Subject's Personal Data from its records upon direction of Customer and shall effect all such deletions within 10 days of receipt of a request.

3.3. In the event that Clario receives a Data Subject request directly from a Data Subject (a "**Direct Access Request**"), Clario shall notify Customer of the request and provide any information or assistance requested by Customer. Clario shall to the extent legally permitted, not act directly on the Direct Access Request, and promptly inform the Customer providing full details of the same and provide the Customer with contact details of the Data Subject(s).

4. CLARIO PERSONNEL

4.1. Clario shall ensure that its personnel engaged in the processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Customer Data, including but not limited to the obligations in this DPA.

4.2. Clario will take appropriate steps to ensure compliance with the Security Measures outlined in Part 2 of the Data Processing Schedule by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Clario.

4.3. Clario shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Services.

5. SUBCONTRACTORS/AFFILIATES

5.1. Clario shall not engage a Subcontractor or share Personal Data with an Affiliate in relation to the processing of Customer's Data without the prior written consent of Customer.

5.2. Customer hereby authorizes Clario to appoint the Subcontractors and share with the Affiliates listed in the Data Processing Schedule to Process Customer's Data for the Business Purpose indicated in the Data Processing Schedule. For the avoidance of doubt, Clario may disclose Customer's Data to Subcontractors or Affiliates solely for the purposes for which such Subcontractors or Affiliates are approved.

5.3. Clario shall inform Customer of any intended changes concerning the addition or replacement of Subcontractors or Affiliates at least 30 days before such change is intended to take place.

5.4. In the event that Clario engages a Subcontractor or Affiliate with Customer's consent, Clario shall enter into a written data processing agreement with the Subcontractor or Affiliate containing requirements equivalent to those set forth in this Agreement.

5.5. Notwithstanding the appointment of Subcontractors or Affiliates, Service Provider will remain fully responsible and liable to Business for any breach of its (or its Subcontractors or Affiliates) obligations under this Agreement in relation to the processing of Business's Data.

5.6. Customer acknowledges and agrees that Third Party Partners are not Subcontractors and Clario assumes no responsibility or liability for the acts or omissions of such Third Party Partners. Subcontractors retained by Clario to provide Services for Customer will at all times be deemed Subcontractors of Clario and shall not under any circumstance be construed or deemed to be employees of Clario or Subcontractors of Customer for purposes of this Agreement.

6. DATA SECURITY

6.1. 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 likelihood and severity of any risk, Clario shall maintain administrative, physical and technical safeguards sufficient for protection of the security, confidentiality and integrity of Customer's Personal Data. Clario will implement and maintain

technical and organizational measures ("**Security Measures**") to protect Personal Data against a Security Breach. The Security Measures shall include, at a minimum, measures to encrypt Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Clario's systems and services; to restore timely access to Personal Data following an incident; and for regular testing of effectiveness. Clario may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

6.2. Clario shall maintain throughout the term of this Agreement the data security measures set out in Part 2 of the Data Processing Schedule (as may be improved and modified from time to time in response to changing risks and the availability of security measures, but, in any event, at least equivalent to the requirements of clause 6.1 above and to those measures set out in the Data Processing Schedule).

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1. If Clario becomes aware of a Security Breach, Clario will promptly notify Customer of the Security Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps Clario recommends Customer take to address the Security Breach.

7.2. Customer agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer Personal Data or to any of Clario's equipment or facilities storing Customer Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7.3. Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Clario selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on Clario's support systems at all times.

7.4. Clario's notification of or response to a Security Breach under this Section will not be construed as an acknowledgement by Clario of any fault or liability with respect to the Security Breach.

7.5. Clario shall implement reasonable technical and organizational Security Measures to provide a level of security appropriate to the risk in respect to the Customer's Data. As technical and organizational measures are subject to technological development, Clario is entitled to implement alternative measures provided they do not fall short of the level of data protection set out by the Data Protection Laws.

8. DELETION OF PERSONAL DATA

8.1. Clario will enable Customer to delete Personal Data during the Term in a manner consistent with the functionality of the Services.

8.2. Clario will comply with written requests from the Customer to delete certain Personal Data as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage.

8.3. Within thirty (30) days of expiration of the Agreement, Clario shall, at Customer's option, delete all Personal Data (including existing copies thereof) from Clario's systems and discontinue processing of such Personal Data in accordance with Data Protection Law. Clario will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) or Google Cloud Platform publicly-posted policies and procedures require further storage or a longer deletion cycle. This requirement shall not apply to the extent that Clario has archived Personal Data on back-up systems so long as Clario securely isolates and protects such data from any further processing except to the extent required by applicable law. Without prejudice to this Section, Customer acknowledges and agrees that Customer will be responsible for exporting, before the

Agreement expires, any Personal Data it wishes to retain afterwards. Notwithstanding the foregoing, the provisions of this DPA will survive the termination of this Agreement for as long as Clario retains any of Customer's Data.

9. TERM AND TERMINATION

9.1. This Agreement shall commence upon the commencement of Processing of Customer's Data by Clario for the purpose of the Order(s) and shall continue to have effect for as long as Clario continues to Process Customer's Data pursuant to the Order(s).

9.2. On the expiry or termination of this Agreement, Clario shall follow Customer's explicit written instructions regarding the disposition of all records of Customer's Data in its possession or control, except insofar as it is required to keep such records under Applicable Law in the U.S.

9.3. The termination or expiry of this Agreement shall not affect any provision of this Agreement intended to have effect after termination or necessary for its interpretation, and, in particular, it shall not affect the provisions of clauses 1 (Interpretation), 2.1 (Data Processing roles), and 3 (Co-operation)

DATA PROCESSING SCHEDULE

Part 1 – Data Processing Information Service Provider's name: Clario, Inc**.**

Service Provider's commercial address:
6600 City West Parkway, Ste 100
Eden Prairie, MN 55344

Service Provider's contact person and email/fax:
Contact: Matt Redlon, CEO (matt.redlon@clar.io)
Legal notices: a copy must also be sent to
Terri Krivosha
Maslon LLP
3300 Wells Fargo Center
90 South 7th Street
Minneapolis, 55402

Service Agreement (titles): active Master Subscription Agreement and Order(s)

Nature and purpose of processing (i.e., "Business Purpose"): Marketing Analytics

Commencement Date: as per each Order

Duration of the processing of Personal Data: On Going

Categories of Personal Data to be processed: Customer and Personal data

Categories of Data Subjects whose Personal Data is to be processed: All customers of Customers unless otherwise defined in the Order

Data sources: Customer's internal systems; customer's third-party systems; Clario data collection platform.

Data security requirements: N/A

Permitted Affiliates (including a description of relationship and the purpose of the access to Personal Data given to each affiliate):

Permitted Subcontractors (including a description of the purpose of the access to Personal Data given to each subcontractor):

Part 2 – Security Measures - Details to ensure data security

Clario Security Organization:
Clario has implemented an information security management program headed by the Director of IT Operations under the direction of the Vice President of Engineering. These two roles form the Information Security (Infosec) team. Infosec establishes and reviews the security strategy and approves risk management plans, security policies, and security communication plans. Infosec also reviews and approves changes to the system development methodology as it relates to system security and availability.

Ongoing Risk Assessments:
Clario uses the System and Organization Controls for Service Organizations 2 (SOC 2) framework for evaluating whether our controls and practices are effective at safeguarding the privacy and security of customer and client data. Frameworks employed in whole or in part as the underlying foundation of the risk assessment include ISO 27001 and Center for Information Security (CIS), CIS v7.

Security Incident Response Plan:
Clario has a comprehensive security incident response plan that outlines responsibilities and actions to be performed in the event of a breach of security, both physical and informational. The plan, which is closely modeled after Clario's non-security incident triage process, includes step-by-step procedures for denial of service situations, malicious code exposure, unauthorized access and inappropriate usage. Guidance for incident participants, based on company role, is detailed within the plan. The plan includes an incident runbook, documentation requirements, and guidance on forensic matters as well as communication plans.

Background Checks:
Clario requires extensive background checks for all new employees. Background checks are outsourced to a reputable third party and managed internally by the Human Resources team. Clario requires all contract or temporary workers who may have access to Customer's Data to undergo a background check sourced by the firm by which they are employed.

Encryption Policy:
Clario encrypts all Personal Data in transit and at rest, and maintains a detailed encryption policy coupled with an encryption technology guide defining acceptable technologies. Encryption key access is restricted to the fewest number of custodians needed to operate. Key storage is limited to secure locations, with as little duplication or key storage instances as possible. Systems have fully implemented and documented key generation processes, key distribution processes, key storage details, periodic key change processes and key destruction processes. All new development efforts are required to use approved encryption technologies. New code implementing obsolete or transitional technologies will not be approved for deployment. All Clario systems use TLS for data transmission, or secured RPC connectivity between systems within the Google Cloud fabric. Data is also encrypted at rest within the Google environment under the AES 256 algorithm.

System Privileges:
Each Clario associate is granted the minimum set of privileges to perform their assigned job function ("Least Privilege Access"). Least Privilege Access is also employed for any privileged data, as determined by assigned responsibilities. When an associate changes roles within the company or is terminated, privileges are reassessed and modified appropriately. The Clario Infosec team is responsible for coordinating timely cancellation of privileges in the event of the termination of an employee. All privileges are reviewed on the Clario platforms and related tools on a quarterly basis.

Data Retention Policy:
Clario maintains a detailed data retention policy for all categories of data stored within Clario's processing facilities. Customer Data is stored for the term of the business relationship. Data for active Customers is stored for 5 years prior to being purged unless an alternative retention period has been arranged with the Customer.

Data Destruction Policy:

Clario has strict data destruction policies. All Customer Data resides in a multi-tenant secure cloud storage system. Data is destroyed upon Customer request or within 30 days of termination of an Agreement if a new Agreement is not executed.

Intrusion Detection:
Clario makes use of Amazon Web Service's intrusion detection capabilities which include sophisticated data processing pipelines which integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security and operational personnel warnings of possible incidents.