Customer Data Processing Addendum

This data processing addendum ("**DPA**") is effective as of the last signature date of an Order and is between Medallia, Inc. ("**Medallia**") and the other signatory to the Order ("**Customer**"). Medallia and Customer are parties to a Medallia Master Subscription Agreement (including any Statement of Work, Program Statement, Product Description, Order Form, or other agreements between the parties, collectively the "**Underlying Agreements**").

This DPA supplements the Underlying Agreements and establishes that Medallia and its subsidiaries will process Personal Data on behalf of Customer and its Affiliates that are authorized to use the experience management products that Medallia provides to Customer (the "**Medallia Products**") under the Underlying Agreements. All capitalized terms not defined in this DPA shall have the meanings set forth in the Underlying Agreements.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**CCPA**" means the California Consumer Privacy Act of 2018.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

"**Customer Data**" means any Personal Data that Medallia processes on behalf of Customer as a Data Processor in the course of providing the Medallia Products and Services, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Underlying Agreements, including, where applicable, the California Consumer Privacy Act of 2018, EU Data Protection Law and UK Data Protection Law.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

"**EU Data Protection Law**" means Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**").

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"**Group**" means any and all Affiliates that are part of an entity's corporate group.

"Model Clauses" means the controller-to-processor standard data protection clauses currently in force, as approved (i) by the Information Commissioner's Office or under applicable UK law, and/or (ii) by the European Commission (as applicable) as amended or updated from time to time).

"**Personal Data**" means information relating to an identified or identifiable natural person.

"**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, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.

"**Security Incident**" means any confirmed unauthorized or unlawful breach of security that leads to the destruction, loss, alteration, or unauthorized disclosure of or access to Customer Data.

"**Sell**" (and its derivatives), and "**Service Provider**" shall have the meaning ascribed to them in the CCPA or the meaning ascribed to those terms or similar terms in any other similar law, as applicable.

"**Special Category Personal Data**" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**Services**" means the professional services provided by Medallia to Customer under the Underlying Agreements.

"**Sub-processor**" means any Data Processor engaged by Medallia or its Affiliates to assist in fulfilling its obligations with respect to providing the Medallia Products and Services pursuant to the Underlying Agreements or this DPA. Sub-processors may include third parties or Medallia Affiliates.

"**UK Data Protection Law**" means the Data Protection Act 2018, Privacy and Electronic Communications (EC Directive) Regulations 2003, and 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 as implemented into UK law (United Kingdom General Data Protection Regulation) (as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020) ("**UK GDPR**").

2. Roles and Scope of Processing

2.1 **Role of the Parties.** As between Medallia and Customer, Customer is the Data Controller of Customer Data and Medallia shall process Customer Data only as a Data Processor or Service Provider acting on behalf of Customer.

2.2 **Medallia's Processing of Customer Data; No Sale.** Medallia shall process Customer Data in compliance with Data Protection Laws. Medallia shall not (i) Sell Customer Data, or (ii) retain, use, or disclose the Customer Data for any purpose other than for the

specific purpose of performing the services specified in the Underlying Agreements and this DPA.

2.3 **Customer Processing of Customer Data.** Customer shall ensure that Medallia's processing of Customer Data is permitted under applicable Data Protection Laws. This obligation includes: (i) complying with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Medallia; and (ii) ensuring that Customer's privacy policy allows for the delivery of Customer Data to Medallia and its use as disclosed to Customer by Medallia; (iii) securing any required consents and rights necessary under Data Protection Laws for Medallia to process Customer Data and provide the Medallia Products and Services pursuant to the Underlying Agreements and this DPA; and (iv) informing Medallia in a timely manner of any opt out requests received after the delivery of the Customer Data.

2.4 **Customer Instructions.** Medallia shall process Customer Data only in accordance with Customer's documented lawful instructions. The parties agree that this DPA, the Underlying Agreements, any actions taken by Customer in the Medallia Products, and any instructions related to Services, set out the Customer's complete instructions to Medallia in relation to the processing of Customer Data. Additional processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Medallia.

2.5 **Details of Data Processing.** The subject matter, duration, purpose of processing, categories of data subjects and types of personal data are set out in Annex A.

2.6 **Access or Use.** Medallia will not process Customer Data, except as necessary (i) to provide or maintain the Medallia Products, provide Services, or other obligations in the Underlying Agreements; or (ii) to comply with the law or binding order of a governmental body.

2.7 **Prohibited Data.** Customer shall not configure the Medallia Products to collect any bank account numbers or bank transaction information, payment card or credit card information, social security numbers, state identification numbers, passports numbers, and Special Category Personal Data (collectively, "**Prohibited Data**"). Where Prohibited Data is nevertheless submitted within Customer Data, Customer acknowledges that in such cases Medallia will not be responsible for any subsequent liability arising from the processing of the foregoing categories of data.

3. Subprocessing

3.1 **Authorized Sub-processors.** Customer agrees that Medallia may engage Sub-processors to process Customer Data on Customer's behalf, and authorises (a) Medallia to appoint other members of the Medallia Group as sub-processors, and (b) Medallia and other members of the Medallia Group to appoint third party data centre operators, servicing, analytics and technical support providers, technology and software providers, and outsourced support providers as sub-processors to support the performance of the Services.

3.2 **Sub-processor Obligations.** Medallia shall: (i) enter into a written agreement with the Sub-processor as required by Article 28 of GDPR or UK GDPR (as applicable) (or their equivalent in Data Protection Laws); and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Medallia to breach any of its obligations under this DPA.

3.3 **Changes in Sub-Processors for Medallia Products.** For Sub-processors that are used to provide the Medallia Products:

(a) Medallia shall inform Customer in advance (by email or by posting on the company website) of any intended new or replacement sub-processors prior to them starting sub-processing Customer Data.

(b) Customer may object to Medallia's appointment of a new Sub-processor by sending an email to privacy@medallia.com within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution.

4. Security

4.1 **Security Measures.** Medallia shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Medallia's security standards described in Annex B ("**Security Measures**").

4.2 **Updates to Security Measures.** Customer is responsible for reviewing the information made available by Medallia relating to data security and making an independent determination as to whether the Medallia Products and Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Medallia 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 purchased by the Customer.

4.3 **Confidentiality of Processing.** Medallia shall ensure that any person who is authorized by Medallia to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (including contractual or statutory duties).

4.4 **Security Incident Response.** Upon becoming aware of a Security Incident, Medallia shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Medallia shall promptly take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

4.5 **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Medallia Products, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Medallia Products and taking any appropriate steps to securely encrypt and transfer any Customer Data to the Medallia Products, as well as backup information before uploading it to the Medallia Products.

5. Security Reports and Audits

5.1 Customer acknowledges that certain Medallia Products are regularly audited against SSAE 16 (SOC 2 Type 2) and/or ISO27001 standards by independent third party auditors and/or internal auditors. Upon request, Medallia shall supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Customer where available, so that Customer can verify Medallia's compliance with the audit standards against which it has been assessed, and this DPA.

5.2 Medallia shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security

and audit questionnaires that are necessary to confirm Medallia's compliance with this DPA, provided that Customer will not exercise this right more than once per year.

5.3 While it is the parties intention ordinarily to rely on the provision of the Report and written responses provided under sections 5.1 and 5.2 above to verify Medallia's compliance with this DPA, Medallia shall permit the Customer (or its appointed third party auditors) to carry out an audit of Medallia's processing of Customer Data under the Underlying Agreements following a Security Incident suffered by Medallia or upon the instruction of a data protection authority. Customer must give Medallia reasonable prior notice of such intention to audit, conduct its audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Medallia's operations. Any such audit shall be subject to Medallia's security and confidentiality terms and guidelines.

6. International Transfers

6.1 **Data Center Locations.** Medallia may transfer and process Customer Data anywhere in the world where Medallia, its Affiliates or its Sub-processors maintain data processing operations, which includes the United States, United Kingdom, the European Union, Argentina, Canada, Israel and Australia. Medallia will at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

6.2 **Adequacy decisions and Model Clauses.** To the extent that Medallia processes any Customer Data protected by EU Data Protection Law or UK Data Protection Law or that originates from the EEA or UK under the Underlying Agreements, and the processing occurs in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority or UK Secretary of State and/or UK Information Commissioner's Office (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Medallia will be deemed to have adequate protection (within the meaning of EU Data Protection Law or UK Data Protection Law (as applicable)) by Medallia complying with the Model Clauses. Under the Model Clauses, Medallia will be a "data importer" and Customer will be the "data exporter" (even if Customer is an entity locating outside the EEA). Medallia will inform Customer if Medallia is unable to comply with the requirements of this section 6.

6.3 **Alternative Transfer Mechanism.** The parties agree that the data export solutions identified in section 6.2 will not apply if and to the extent that Medallia adopts an alternative data export solution for the lawful transfer of Personal Data (as recognised under EU Data Protection Laws) outside of the EEA and which Medallia makes available on its website including binding corporate rules, in which event, that mechanism will apply instead (but only to the extent such mechanism extends to the territories to which Personal Data is transferred).

6.4 Medallia may replace the Model Clauses with any alternative or replacement standard contractual clauses approved by the European Commission and/or or UK Secretary of State and/or UK Information Commissioner's Office (as applicable) by notifying Customer of the new Model Clauses and any required changes to the Appendices to the Model Clauses (by email, or, if applicable, by posting on its website), provided that such updates are in compliance with the relevant decision or approval.

7. Return or Deletion of Data

7.1 Upon termination or expiration of the Underlying Agreements, Medallia shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control in accordance with this section 7.

7.2 For thirty (30) days following termination or expiry of the Underlying Agreements (the "**Data Transfer Period**"), Medallia will allow Customer to retrieve or delete any remaining Customer Data from the Medallia Products, subject to the terms and conditions set out in the Underlying Agreements. Within sixty (60) days of the end of the Data Transfer Period, Medallia will remove all personally identifiable program data from its systems.

7.3 Section 7.2 shall not apply to the extent Medallia is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Data.

8. Data Subject Requests; Cooperation

8.1 To the extent that Customer is unable to independently use Medallia's processes or controls to retrieve, correct, delete or restrict Customer Data in connection with Customer's obligations under the CCPA, EU Data Protection Law or UK Data Protection Law (as applicable), Medallia shall provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Underlying Agreements. In the event that any such request is made directly to Medallia, Medallia shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Medallia is required to respond to such a request, Medallia will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 If a law enforcement agency sends Medallia a demand for Customer Data (for example, through a subpoena or court order), Medallia will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Medallia may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Medallia will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Medallia is legally prohibited from doing so.

8.3 To the extent Medallia is required under Data Protection Laws, Medallia shall provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. General

9.1 The parties agree that this DPA shall replace any existing DPA (including the Model Clauses, as applicable) the parties may have previously entered into in connection with the Medallia Products and Services.

9.2 Except for the changes made by this DPA, the Underlying Agreements remains unchanged and in full force and effect. If there is any conflict between this DPA and the Underlying Agreements, this DPA shall prevail to the extent of that conflict.

9.3 Any claims brought under the Model Clauses or this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Underlying Agreements. Any regulatory penalties incurred by Medallia in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws will count toward and reduce Medallia's liability under the Underlying Agreements as if it were liability to the Customer under the Underlying Agreements.

9.4 Any claims against Medallia or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Underlying Agreements. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

9.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Underlying Agreements, unless required otherwise by applicable Data Protection Laws.

9.6 This DPA and the Model Clauses will terminate simultaneously and automatically with the termination or expiry of the Underlying Agreements.

Annex A – Description of processing

(a) **Subject Matter:** The subject matter of the data processing under this DPA is the Customer Data.

(b) **Duration:** The duration of the data processing under this DPA is until the termination or expiration of the Underlying Agreements in accordance with its terms.

(c) **Purpose:** The purpose of the data processing under this DPA is the provision of the Medallia Products and Services to the Customer and the performance of Medallia's obligations under the Underlying Agreements or as otherwise agreed by the parties.

(d) **Nature of the Processing:** Medallia provides the Medallia Products, which enables Customer to collect, analyze and respond to feedback from its customers, and related Services as described in the Underlying Agreements. Medallia processes Customer Data upon the instruction of the Customer in accordance with the terms of the Underlying Agreements.

(e) **Categories of Data Subjects:** Medallia processes Personal Data relating to the following categories of data subjects:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors;

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons); and

(iv) Customer's end-users authorized by Customer to use the Medallia Products.

(f) **Types of Personal Data:** Customer may submit Personal Data to the Medallia Products, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

(i) Identification and contact data of those data subjects who will provide feedback or other signals or take surveys (e.g., name, address, title, contact details);

(ii) Identification, contact data, and role information of data subjects who will access the Medallia Products (e.g., name, address, title, contact details, employer, job title, job location, area of responsibility);

(iii) Touchpoint information for those data subjects who will provide feedback or other signals or take surveys (e.g., transaction identifier, location visited);

(iv) IT information of data subjects who will provide feedback or other signals or take surveys or access the Medallia Products (e.g., IP addresses, cookies data); and

(v) Other categories of data Customer may choose to send to Medallia or collect through the Medallia Products (e.g., open-ended experience feedback, ideas, video feedback, reward program membership).

(g) **Special category Personal Data (if applicable):** None.

Annex B – Security Measures

Medallia maintains and manages a comprehensive written security program designed to protect: (a) the security and integrity of Customer Data; (b) against threats and hazards that may negatively impact Customer Data; and (c) against unauthorized access to Customer Data. Medallia's security program includes the following:

1. Risk Management

a. Conducting an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used in the Medallia Products.

b. Maintaining a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.

2. Information Security Program

a. Maintaining a documented comprehensive information security program. This program will include policies and procedures aligning with industry best practices, such as ISO 27001/27002.

b. Such information security program shall include, as applicable: (i) adequate physical security of all premises in which Customer Data will be processed and/or stored; (ii) reasonable precautions taken with respect to Medallia personnel employment; and (iii) an appropriate network security program.

c. These policies will be reviewed and updated by Medallia management annually.

3. Organization of Information Security

a. Assigning security responsibilities to appropriate Medallia individuals or groups to facilitate protection of the Medallia Products environment and associated assets.

b. Establishing information security goals to be met.

4. Human Resources Security

a. Medallia employees undergo comprehensive screening during the hiring process. Background checks and reference validation will be performed to determine whether candidate qualifications are appropriate for the proposed position. Subject to any restrictions imposed by applicable law and based on jurisdiction, these background checks include criminal background checks, employment validation, and education verification as applicable.

b. Ensuring all Medallia employees are subject to confidentiality and non-disclosure commitments before access is provisioned to Medallia Products and/or Customer Data.

c. Ensuring applicable Medallia employees receive security and privacy awareness training designed to provide such employees with information security knowledge to provide for the security, availability, and confidentiality of Customer Data.

d. Upon Medallia employee separation or change in roles, Medallia shall ensure any Medallia employee access is revoked in a timely manner and all Medallia assets, both information and physical, are returned.

5. Asset Management

a. Maintaining asset and information management policies and procedures. This includes ownership of assets, an inventory of assets, classification guidelines, and handling standards pertaining to Medallia assets.

b. Maintaining media handling procedures to ensure media containing Customer Data is encrypted and stored in a secure location subject to strict physical access controls.

c. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent Customer Data from being exposed to unauthorized individuals using the techniques recommended by NIST to

destroy data as part of the decommissioning process.

d. If a hardware device is unable to be decommissioned using these procedures, the device will be virtually shredded, degaussed, purged/wiped, or physically destroyed in accordance with industry-standard practices. Devices used in the administration of the Medallia Products that have been decommissioned will be subjected to these or equally effective standards.

6. Access Controls

a. Maintaining a logical access policy and corresponding procedures. The logical access procedures will define the request, approval and access provisioning process for Medallia personnel. The logical access process will restrict Medallia user (local and remote) access based on the principle of least privilege for applications and databases. Medallia user access recertification to determine access and privileges will be performed periodically. Procedures for onboarding and off-boarding Medallia personnel users in a timely manner will be documented. Procedures for Medallia personnel user inactivity threshold leading to account suspension and removal threshold will be documented.

b. Limiting access to Customer Data to its personnel who have a need to access Customer Data as a condition to Medallia's performance of the services under this Agreement. Medallia shall utilize the principle of "least privilege" and the concept of "minimum necessary" when determining the level of access for all Medallia users to Customer Data. Medallia shall require strong passwords subject to complexity requirements and periodic rotation.

7. System Boundaries

a. The systems that compose a functioning Medallia cloud platform for the Products are limited to shared components such as network devices, servers, and software that are physically installed and operating within Medallia's Internet-enabled network infrastructure. This system boundary also includes the network connectivity, power, physical security, and environmental services provided by the third-party provider that owns and operates the data centers in which this network infrastructure is collocated.

b. Medallia is not responsible for any system components that are not within this system boundary, including network devices, network connectivity, workstations, servers, and software owned and operated by the Customer or other third parties. Medallia may provide support for these components at its reasonable discretion.

8. Encryption

a. Customer maintains ownership of the encryption all Customer Data uploaded to their Products through the full lifecycle period. Customer Data may be uploaded via SFTP, TLS/SSL, or through an Medallia services API over a TLS/SSL connection to the Medallia cloud platform. Medallia will configure TLS and/or SSL certificates.

b. Customer Data shall be encrypted at rest at the storage-level.

9. Physical and Environment Security

a. Medallia products and customer data are hosted at providers who have demonstrated compliance with one or more of the following standards (or a reasonable equivalent): International Organization for Standardization ("ISO") 27001 and/or American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC") Reports for Services Organizations. These providers provide Internet connectivity, physical security, power, and environmental systems and services for the Medallia cloud platform used for the Products.

b. An N-tiered architecture is used to support presentation, application, processing, and data services. For enhanced security in the Medallia cloud platform, technologies such as firewalls, intrusion detection and prevention, and vulnerability management are used.

10. Operations Security

a. Maintaining documented Medallia cloud operating procedures.

b. Maintaining a defined process for the controlled, authorized release of product changes.

c. Utilizing virus and malware protection software a, which are configured to meet common industry standards designed to protect Medallia systems and Customer Data from virus infections or similar malicious payloads.

d. Implementing disaster recovery and business continuity procedures. These will include periodic replication of Customer Data to a secondary data center in a geographically disparate location from the primary data center.

e. Ensuring systems processing and storing customer data are appropriately configured and hardened.

f. Ensuring servers, operating systems, and supporting software used in the Medallia cloud for Products receive Critical and High security patches within a timely manner, In the event any such security patch would materially adversely affect the Products, then Medallia will use commercially reasonable efforts to implement compensating controls until a security patch is available that would not materially adversely affect the Products.

g. Conducting third-party external application penetration tests periodically.

11. Supplier Relationships

a. Maintaining a Vendor Management Program to evaluate and mitigate risks for any third-parties that host or process customer data.

12. Security Incident

a. Employing incident response standards that are based upon applicable industry standards, such as ISO 27001:2013 and National Institute for Standards and Technology ("NIST"), or equivalent in order to maintain the information security components of the Products environment.

b. Responses to these incidents follow the Medallia documented incident response sequence. This sequence includes the incident trigger phase, evaluation phase, escalation phase, response phase, recovery phase, de-escalation phase, and post-incident review phase.

13. Information Security Aspects of Business Continuity Management

a. Maintaining a business continuity and disaster recovery plan.

b. Reviewing and testing this plan annually.