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 and EU 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 standard contractual clauses for Processors as approved by the European Commission and available at http://ec.europa.eu/ (as amended or updated from time to time). Annex B sets forth the appendices to the Model Clauses.

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

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Processing**" has the meaning given to it in the GDPR 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.

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

"**Sensitive 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.

"**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 members of the Medallia Group.

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 providing the Medallia Products and performing the services specified in the Underlying Agreements and this DPA (except to comply with the law or binding order of a governmental body).

2.3 **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 and final 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.

2.4 **Details of Data Processing.**

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

(b) Duration: As between Medallia and Customer, the duration of the data processing under this DPA is until the termination 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: Medallia processes the following types of Personal Data:

(i) Identification and contact data of those data subjects who will provide feedback or other signals (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 (e.g., transaction identifier, location visited);

(iv) IT information of data subjects who will provide feedback or other signals 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) Sensitive Personal Data (if applicable): None.

3. Subprocessing. Customer agrees that Medallia may engage Sub-processors to process Customer Data on Customer's behalf as described at www.medallia.com/subprocessors

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 A ("**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 **Customer Responsibilities**. Customer shall 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.** Medallia shall make available summary copies of audit reports for Medallia Products where available. Additionally, Customer shall have audit rights as specified in the Underlying Agreements.

6. **International Transfers**

6.1 **Data Center Locations**. Customer permits Medallia to transfer and process Customer Data in the countries described at medallia.com/subprocessors.

6.2 **Model Clauses**. To the extent that Medallia processes any Customer Data protected by EU Data Protection Law or that originates from the EEA 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 (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 Legislation) by Medallia complying with the Model Clauses.

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, 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).

7. **Data Subject Requests; Cooperation**

7.1 To the extent that Customer is unable to independently use Medallia's processes or controls to retrieve, correct, delete or restrict Customer Data which Customer may use to assist it in connection with its obligations under Data Protection Laws, 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.

7.2 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.

7.3 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.

8. Relationship with the Underlying Agreements

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

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

Annex A – Security Measures

Medallia has implemented and maintains a security program in accordance with industry standards, which shall include:

ACCESS CONTROL OF PROCESSING AREAS

Suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment, namely the database and application servers and related hardware, where the Personal Data are Processed. This is accomplished by:

- establishing secure areas;
- protection and restriction of access paths;
- securing the data processing equipment and personal computers;
- establishing access authorizations for employees and third parties;
- identification of the personnel with access authority;
- restrictions on card-keys;
- logging, monitoring and tracking all access, including visitors; and
- implementing a security alarm system or other appropriate security measures.

ACCESS CONTROL TO DATA PROCESSING SYSTEMS

Suitable measures to restrict access to personal data to only those Medallia personnel with such authorization; prevent any access to Personal Data and data processing systems from unauthorized persons. This is accomplished by:

- ensuring that access to the systems is limited to those personnel who require such access to provide the Medallia Products;
- requiring authorized personnel to use passwords;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic log file of events, monitoring of unauthorized access attempts;
- employee policies and training in respect of each employee's access rights to the Personal Data;
- logging user access to Personal Data;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

AVAILABILITY CONTROL

Suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy; and
- backups of production data stored at an alternate site, and available to restore in case of failure of the primary system.

TRANSMISSION CONTROL

Suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of adequate firewall and encryption technologies to protect the public gateways through which the data travels; and

INPUT CONTROL

Suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data, as well as for the alteration and deletion of stored data;
- authentication of the authorized personnel;
- utilization of passwords;
- providing that entries to data processing facilities (the data centers housing the computer hardware and related equipment) are capable of being locked; and
- automatic log-off of user ID's that have not been used for a substantial period of time; and proof established within Medallia's organization of the input authorization.

SEPARATION OF PROCESSING FOR DIFFERENT PURPOSES

Suitable measures to ensure that data collected for different purposes can be Processed separately. This is accomplished by:

- separation of Personal Data of different customer programs; and
- separation of access to Personal Data via application security controls.

JOB CONTROL

Suitable measures to ensure that Personal Data is Processed in accordance with the instructions of Customer. This is accomplished by:

- policies, training and monitoring regarding system use and program modifications;
- appointment a security officer who will act as a point of contact for Customer, and coordinate and control compliance with security measures; and

personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements, and such confidentiality obligations survive the termination of the personnel engagement.

Annex B - Appendices to Model Clauses

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer*:* The data importer is the US headquartered company, Medallia, Inc ("**Medallia**"). Medallia is a provider of a customer experience management products offered via a Software-as-a-Service model ("**Medallia Products**") which enables data exporter to collect, analyze and respond to feedback from its customers.

Description of Data Processing: Please see Section 2.4 (Details of Data Processing) of this DPA for a description of the data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Annex A of this DPA, which describes the technical and organisational security measures implemented by Medallia.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in section 3 (Sub-processing) of the DPA.