Customer Data Processing Addendum

The 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"**CCPA**" means the California Consumer Privacy Act of 2018, as amended, superseded or updated from time to time.

"**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, and that is protected as "personal data", "personal information", "personally identifiable information" under Data Protection Laws, 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 without limitation, as applicable, the California Consumer Privacy Act of 2018, the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the EU General Data Protection Regulation, and other applicable privacy and data protection laws.

"**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.

"**European Data Protection Law**" means (i) 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**"); (ii) the EU e-Privacy Directive (2002/58/EC); (iii) any national data protection laws made under or pursuant to (i) or (ii); (iv) UK Data

Protection Law; and (v) the Swiss Federal Data Protection Act ("**Swiss DPA**"), in each case as superseded, amended or replaced..

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

"Model Clauses" means the (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on 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 ("**EU SCCs**"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the United Kingdom Data Protection Act 2018 ("**UK Addendum**"), and (iii) where the Swiss DPA applies, the applicable standard contractual clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner ("**Swiss SCCs**").

"**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.

"**Restricted Transfer"** means (i) where the GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission, (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 and (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not subject to an adequacy decision by the Swiss Federal Data Protection and Information Commissioner.

"**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. A "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“**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 GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**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. Medallia certifies that it understands and will comply with the requirements and restrictions set out in Section 2.2 and will comply with the requirements applicable to Service Providers under the CCPA.

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 other applicable 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 (where Customer has signed up to receive notification of updates via the link on the Medallia Subprocessor List webpage, which will be communicated via email and by posting on the company website) of any intended new or replacement sub-processors two (2) weeks 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 18 (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, upon written request from Customer, provide Customer with a copy of the relevant industry standard security certifications obtained by Medallia ("Security Certifications") and any available Medallia's responses to industry recognized questionnaires related to security and audit such as CAIQ and SIG ("Industry Questionnaires"). Customer agrees and acknowledges that the Security Certifications and Industry Questionnaires are sufficient to confirm Medallia's compliance with this DPA, but in the event where Customer requires additional written responses to security and audit questionnaires from Medallia that are reasonably necessary to determine Medallia's DPA compliance ("Additional Responses"), Medallia shall issue such Additional Responses to Customer accordingly. For the avoidance of doubt, the Security Certifications, Industry Questionnaire and Additional Responses are provided to Customer on a confidential basis and 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 Transfers.** Customer may choose to have Customer Data stored in a region(s) offered by Medallia. Notwithstanding the foregoing, Medallia will only process and transfer Customer Data outside of the selected region(s) as reasonably necessary to provide the Service (e.g., to provide support, secure, or maintain the Service). Medallia will ensure that any such processing and transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

6.2 **Model Clauses.** The parties agree that when the transfer of Customer Data from Customer (as data exporter) to Medallia (as data importer) is a Restricted Transfer such transfers shall be subject to the appropriate Model Clauses as follows:

(a) in relation to transfers of Customer Data that are protected by the GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, option 2 (*general authorisation to appoint subprocessors*) will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Clause 3.3(a) of this DPA;

(iv) in Clause 11 (*alternative dispute resolution mechanism*), the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA;

(viii) Subject to Section 4.2 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA;

(b) in relation to transfers of Customer Data that are protected by the UK GDPR, the UK Addendum will apply completed as follows:

(i) The EU SCCs, completed above in paragraph (a) of this DPA shall also apply to the transfers of such Customer Data, subject to sub-clause (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the option "importer" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA;

(c) In relation to transfers of Customer Data that are protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

(i) any references in the EU SCCs to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) any references to "EU", "Union" and "Member State law" shall be interpreted as references to Swiss law;

(iii) and any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland, unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Data in compliance with the Swiss DPA, in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. For the purposes of the Swiss SCCs, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in the Annexes I and II to this DPA (as appropriate) and the interpretive provisions set out in this section 6.2(c) shall apply (as applicable and as required for the purposes of complying with the Swiss DPA).

(d) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Model Clauses and, accordingly, if and to the extent the Model Clauses conflict with any provision of the Underlying Agreements or this DPA the Model Clauses shall prevail to the extent of such conflict;

6.3 **Alternative Transfer Mechanism.** The parties agree that the data export solutions identified in section 6 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 applicable European Data Protection Laws) and which Medallia makes available on its website, 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, the UK Secretary of State and/or UK Information Commissioner's Office, or the Swiss Federal Data Protection and Information Commissioner (as applicable) by notifying Customer of the new Model Clauses, replacement standard contractual clauses, or similar and any required changes or additions 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 or European 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 Customer 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 any 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. For the avoidance of doubt, nothing in this DPA is intended to limit the parties' direct liability towards data subjects, including as provided for or permitted under the applicable Model Clauses.

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

LIST OF PARTIES

Data exporter(s): Customer Entity as described in the Underlying Agreement ('Customer')

1. Name: Customer

   Address: The Address is as set out in the Underlying Agreement

   Contact person's name, position and contact details: The Contact Details are as set out in the Underlying Agreement

   Activities relevant to the data transferred under these Clauses: As set out in the Underlying Agreement between the parties.

   Signature and date: _____

   Role (controller/processor): Controller

Data importer(s):

1. Name: Medallia Inc.

   Address: 6220 Stoneridge Mall Rd, Floor 2, Pleasanton, CA 94588, United States

   Contact person's name, position and contact details: privacy@medallia.com

   Activities relevant to the data transferred under these Clauses: As set out in the Underlying Agreement between the parties.

   Signature and date: _____

   Role (controller/processor): Processor

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

(a) 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.

Categories of personal data transferred

(b) 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).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (eg. whether the data is transferred on a one-off or continuous basis).

Continuous

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.

Purpose(s) of the data transfer and further processing

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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the data processing under this DPA is until the termination or expiration of the Underlying Agreements in accordance with its terms.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the Processing of Personal Data by (Sub) Processors, if applicable, shall be as outlined above.

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Irish Data Protection Authority

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:

Technical and Organizational Security Measures	**Evidence of Technical and Organizational Security Measures**
Measures of encryption of Customer Data	All Customer Data by default is encrypted in transit and at rest. Information is always transmitted over the Internet via TLS with up-to-date encryption methodologies.

Measures for ensuring ongoing confidentiality and availability of processing systems and services	**Confidentiality:** Data protection is a top priority for Medallia and we treat all Customer Data as private and sensitive. Medallia enters into agreements that contain confidentiality provisions with our employees, contractors, vendors and Sub Processors for safe measures. Customer Data is only processed to provide the service agreed-upon and no data is shared with third parties without the approval of the Customer. Our customers are in control of their data. We have standard, industry compliant policies for deletion and retention of data that our customers can use, but they can opt for stronger requirements. Our customers are the Data Controller and Medallia is the Data Processor. Additionally, Medallia maintains strict policies and procedures for classifying and securing client data. Our data classification policy defines these classifications and associated handling requirements, including: labelling, encryption, transmission, data transfer, processing, security safeguards, and deletion. Personnel are prohibited from copying or storing client data onto removable media or mobile devices. Medallia also enforces a clear desk/clear screen policy. Furthermore, Medallia has instituted policies and procedures for the acceptable use of electronic resources. These policies cover confidentiality and security of email messages, prohibit the use of illegal software, and provide guidance on the acceptable use of social media and other public communications media. **Availability:** Medallia's Business Continuity Plan (BCP) supports continued delivery of its products and services after a disaster event that impacts the resources required (i.e., people, technology, physical assets and/or relationships) to support the performance of its critical business processes. The scope of the BCP includes business continuity procedures for Medallia's global teams that support delivery of Medallia's products and services. Medallia has also established a Crisis Management Plan to supplement the BCP and prepare for a crisis that may involve technology, business, natural, human, and regulatory events, and includes participation from Medallia staff, counsel, government, public relations, board of directors, and shareholders. Medallia products are hosted in data centers with high resiliency and fully redundant network and communication infrastructure. Our infrastructure and client data is stored at Tier III, SOC 2 Type II certified data centers. The data centers offer a complete range of redundant power and communications, including multiple communications, backup diesel generators, raised floors, and 24/7 physical security. Medallia performs regular backups of Customer Data to locations geographically distanced from the primary hosting location. Annual Disaster Recovery tests are conducted to ensure that disaster

	recovery procedures are completely documented and backup restoration can be executed safely in the event of a disaster.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	The goal of Medallia's technical and organizational measures is to protect the confidentiality, security and integrity of the Customer Data and to minimize the risk of damage occurring by preventing Security Incident and managing security threats and vulnerabilities. Our Legal team, Data Protection Officer, and Security team make sure that applicable regulations and standards are factored into our security frameworks. A **"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. A Security Incident shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. Medallia will notify Customer of a Security Incident as required pursuant to applicable law but in no event later than 72 hour after a Security Incident. **Information Security Program:** Medallia maintains a documented comprehensive information security program. This program includes policies and procedures aligning with good industry practices, such as ISO 27001/27002 and has, 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. These policies will be reviewed and updated by Medallia management annually. **Security Certifications:** Medallia undergoes regular independent reviews of its security and privacy program, which may include the following certifications and activities depending on the products and/or services purchased: ● HITRUST CSF; ● FedRAMP; ● SOC 2 Type 2; ● ISO 27001; ● Third-party penetration testing; and/or ● Other attestations as applicable.

Measures for user identification and authorisation	Medallia limits 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 the Agreement. Medallia utilizes the principle of "least privilege" and the concept of "minimum necessary" when determining the level of access for all Medallia users to Customer Data. By default, Medallia requires strong passwords subject to complexity requirements periodic rotation, Single Sign-On (SSO), and Multi-factor Authentication (MFA). **Access Control of Processing Areas:** Measures to prevent unauthorized persons from gaining access to the database and application servers and related hardware, where the Customer Data are processed: ● 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 of Data Processing Systems** Measures to restrict access to Customer Data to only those Medallia personnel with such authorization: ● 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 Customer Data; ● logging user access to Customer Data;

	● control of files, controlled and documented destruction of data; and ● policies controlling the retention of back-up copies. **Input Control** Measures to ensure that it is possible to establish whether and by whom Customer Data have been input or removed: ● an authorization policy for the input, alteration and deletion of stored data; ● authentication of the authorized personnel; ● use of passwords; ● providing that entries to the data centers housing the computer hardware and related equipment are capable of being locked; and ● automatic log-off of user IDs that have not been used for a substantial period of time. **Separation of Processing for Different Purposes** Measures to ensure that data collected for different purposes can be processed separately: ● separation of Customer Data of different customer programs; and ● separation of access to Customer Data via application security controls.

Measures for user identification and authorisation	**Job control [relating to partner communications]** Where applicable, measures to ensure that Customer Data is processed in accordance with the instructions of Customer communicated to Medallia through Customer's authorized partner ("Partner"): ● policies, training and monitoring regarding system use and program modifications; ● personnel engaged in the processing of Customer Data are informed of the confidential nature of the Customer Data, have received appropriate training on their responsibilities and the relevant privacy regulations; and ● executed written confidentiality agreements with confidentiality obligations, including not to use such Customer Data for any purpose except for providing Medallia Products to Partner and Customer, that survive the termination of the personnel engagement. Medallia maintains a logical access policy and corresponding procedures. The logical access procedures define the request, approval and access provisioning process for Medallia personnel. The logical access process restricts Medallia user (local and remote) access based on the principle of least privilege for applications and databases. Medallia user access recertification access and privileges will be performed periodically. Procedures for onboarding and off-boarding Medallia personnel users in a timely manner are documented. Procedures for Medallia personnel user inactivity threshold leading to account suspension and removal threshold are documented.

Measures for the protection of data during transmission	**Transmission Control** To prevent the Customer Data from being read, copied, altered or deleted by unauthorized parties during the data transmission, Medallia uses firewall and encryption technologies to protect the public gateways through which the data travels. Customer Data is exchanged with other platforms in a number of ways, many of which are enabled by our Auto-Importer, namely a suite of record handling and ETL tools that automate data transfer and manipulation. This offers Customers greater flexibility and eliminates manual errors in data transmission processes. Medallia utilizes TLS 1.2 for secure data transmission between the web client and the web server. Access to the Medallia application is only open over HTTPS, which leverages TLS 1.2, to ensure all data, including personally identifiable information, is encrypted in transit. This protects transmissions between the Customer and Medallia Products on all channels including mobile devices. Medallia supports and strongly recommends the use of SFTP protocol for all file exports and imports. SFTP protocol is a platform-independent protocol that provides encrypted communication channels to transfer files between systems. Unlike standard FTP, SFTP encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over a network. For additional data security, Medallia also supports and recommends encrypting data files containing PII using PGP before transmitting them over SFTP. PGP encryption provides security of data at rest, and SFTP provides security of data in transit.
Measures for the protection of data during storage	Medallia has multiple layers of controls for securing stored Customer Data. Customer Data is stored on AES-256 encrypted hard drives. Feed files containing Customer Data can also be encrypted with PGP. Calls to Medallia databases are made using secure Java Database Connectivity (JDBC). Database servers with Customer Data have been hardened based on good industry practices: we turn off unnecessary services, ensure the security packages are updated, and restrict access to the servers to authorized users and services only.
Measures for ensuring physical security of locations at which Customer Data are processed	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 Medallia Products. Physical access to data centers are secured at perimeters and building ingress points by security using video surveillance, intrusion detection mechanisms, and access control systems. Authorized staff must pass multiple factors of authentication (minimum of two (2) times) to access data center floors with Medallia data. All

	visitors and contractors are required to present identification and are signed in, logged, and continually escorted by authorized staff.
Measures for ensuring events logging	Medallia and Customer assets are monitored by Site Reliability Engineering (SRE) and the Trust and Assurance Group (TAG) 24/7, 365 days a year; all relevant user activities, system exceptions and security events are logged and stored in a centralized log management system to prevent tampering. Privileged access is also monitored using a centralized log management solution. Access to logging facilities and log information is restricted to authorized personnel only. Medallia's Security Incident policy enforces the incident response plan and its procedures. These guidelines are followed if any type of security incident occurs.
Measures for ensuring system configuration, including default configuration	Medallia follows a consistent change management process for all the changes to our products' production environments. Changes need to be approved by a designated party and executed according to the formal change control process. The control process ensures that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored. Configuration baselines and hardened immutable images are utilized to securely configure the systems by following good industry-practices.
Measures for internal IT and IT security governance and management	Medallia conducts an annual risk assessment designed to identify threats and vulnerabilities in the administrative, physical, legal, regulatory, and technical safeguards used in the Medallia Products. Additionally, we also maintain a documented risk remediation process to assign ownership of identified risks, establish remediation plans and timeframes, and provide for periodic monitoring of progress.
Measures for certification/assurance of processes and products	Medallia undergoes regular independent reviews of its security and privacy program, which may include the following certifications and activities depending on the products and/or services purchased: ● HITRUST CSF; ● FedRAMP; ● SOC 2 Type 2; ● ISO 27001; ● Third-party penetration testing; and/or ● Other attestations as applicable.

Measures for ensuring data minimisation	Medallia processes Customer Data for the purposes of the Services and shall only retain Customer Data for: (i) a period of time Customer uses the Services Medallia provides to Customer under the Underlying Agreement, (ii) as long as needed to carry out Medallia's legitimate business interest; and (iii) as required to comply with applicable laws.
Measures for ensuring limited data retention	Customer Data is retained for reasons as stipulated in the Measures for ensuring data minimization above. If Customer specifically requests data be purged, it will be securely erased. Customer Data is not stored on removable media. Any media containing client data will be sanitized or physically destroyed, in accordance with NIST SP 800-88 rev 1 Guidelines for Media Sanitization, before the media is reused or disposed. Upon termination of the Underlying Agreement, Medallia will make Customer Data available for secure download by Customer in a standard flat file format for at least thirty days. Within 60 days of the end of this data transfer period, Medallia will remove the Customer Data from the program instance. All data will be either securely erased according to good industry practices, including backups, or the hard drives will be physically destroyed.
Measures for ensuring accountability	Medallia has implemented information security and data protection policies in accordance with applicable laws and undergoes annual assessments such as SOC 2, ISO 27001, ISO 27017, ISO 27018, ISO 27701 and more. We have a dedicated Security team led by a Chief Information Security Officer and an appointed Data Protection Officer.
Measures for allowing data portability and ensuring erasure	Medallia products contain features that allow for the export of Customer Data by the customer and Medallia has processes in place for the deletion of data subject records. Additionally, our designed data minimization practices ensure that data is retained only for the period required to perform the processing. Medallia can also delete, anonymize, or rectify data at the instruction of a Customer.
Technical and organizational measures to be taken by the sub-processor to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the Customer.	Medallia restricts the transfer of data to subprocessors using the following measures: ● requiring data subprocessors to use security measures that are the same as or equally effective as the ones that Medallia commits to; ● assessing subprocessors for security and privacy compliance; and ● requiring subprocessors to sign a data protection agreement and the appropriate standard contractual clauses, limiting the use of data to the purpose for which Medallia has employed the subprocessor.