Customer EU 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 Data Processing Addendum ("**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 Medallia Experience Cloud 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 Experience Cloud 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.

"**Medallia Experience Cloud**" means the customer experience management platform offered via a Software-as-a-Service model.

"Model Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex C**.**

"**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 Experience Cloud 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 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 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 Experience Cloud and Services pursuant to the Underlying Agreements and this DPA; and (iv) timely informing Medallia of any opt out requests received after the delivery of the Customer Data.

2.4 **Customer Instructions**. Medallia will process Customer Data only for the purposes described in this DPA and 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 Experience Cloud, 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.

2.5 **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 Experience Cloud 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 Experience Cloud, 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 Experience Cloud.

(f) Types of Personal Data: Medallia processes the following types of Personal Data:

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

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

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

(iv) IT information of data subjects who will take surveys or access the Medallia Experience Cloud (e.g., IP addresses, cookies data); and

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

(g) Sensitive Personal Data (if applicable): None.

2.6 **Access or Use**. Medallia will not process Customer Data, except as necessary (i) to provide or maintain the Medallia Experience Cloud, 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 Experience Cloud 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 Sensitive 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. The Sub-processors currently engaged by Medallia and authorized by Customer are listed in **Annex A**.

3.2 **Sub-processor Obligations**. Medallia shall: (i) enter into a written agreement with the Sub-processor as required by Article 28 of GDPR and the Privacy Shield Principles; 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 Services**. Medallia shall obtain Customer's prior written consent to use of any Sub-processors that are used to provide Services, such as system integrators or delivery partners.

3.4 **Changes in Sub-Processors for Medallia Experience Cloud**. For Sub-processors that are used to provide the Medallia Experience Cloud:

(a) Medallia shall (i) provide an up-to-date list of the Sub-processors it has appointed in the documentation for the Medallia Experience Cloud (available at https://docs.medallia.com); and (ii) through its administrative portal, notify Customer if it adds or removes Sub-processors at least fifteen (15) days prior to any such changes.

(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 Experience Cloud 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 Experience Cloud, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Medallia Experience Cloud and taking any appropriate steps to securely encrypt and transfer any Customer Data to the Medallia Experience Cloud, as well as backup information before uploading it to the Medallia Experience Cloud.

5. Security Reports and Audits

5.1 Customer acknowledges that the Medallia Experience Cloud is 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, 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, the European Union, Argentina, Canada, Israel and Australia. This will apply even where Customer has agreed with Medallia to host Customer Data in the EEA if such non-EEA Processing is necessary to provide the Services to Customer. 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 **Privacy Shield and 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 (a) Medallia complying with the Model Clauses, and (b) when the data

processing occurs in the US, Medallia having self-certified its compliance with the Privacy Shield and adhering to the Privacy Shield Principles. 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.

6.3 **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. 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.

7.2 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 Experience Cloud, 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 which Customer may use to assist it in connection with its obligations under the GDPR or the CCPA, 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. Relationship with the Underlying Agreements

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 Experience Cloud 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

List of Medallia Sub-processors

The security and data handling practices of each third party subcontractor is evaluated by Medallia's vendor risk management program. In addition, each third party subcontractor agrees to security and data processing agreements that restrict their access, use and disclosure of personal data in compliance with applicable laws, and our security and privacy certifications.

For more information on Medallia's security program, visit https://www.medallia.com/security/.

Servicing and Technical Support

The subcontractors listed provide servicing and technical support for the Medallia Experience Cloud.

Subcontractor Name	Corporate Location	Processing Description
Effective Teleservices Pvt Ltd	India	Medallia Experience Cloud implementation, servicing and technical support.
CX Software Solutions SA de CV	Mexico	Medallia Experience Cloud implementation, servicing, and topic building for text analytics.
Infinit Outsourcing, Inc.	Philippines	Technical support.
Experis US, Inc.	USA	Topic building for text analytics.
Gemseek Consulting Limited	Bulgaria	Medallia Experience Cloud implementation.
SM Technologies Limited	Brazil	Implementation and servicing.
Omega3c S.r.l.	Italy	Implementation and servicing in Italy.
Runroom S.L.	Spain	Implementation and servicing in southern Europe.

Technology Providers

The subcontractors listed provide technology for the Medallia Experience Cloud.

Subcontractor Name	Corporate Location	Processing Description
Sumo Logic, Inc.	USA	Manages system logs for diagnosis and resolution of technical issues.
Salesforce.com, Inc.	USA	Tracks technical support tickets.
Amazon Web Services, Inc.	USA	Archives security logs for security incident monitoring and detection. Hosts and processes data for Medallia for Digital and Strikedeck. Renders front-end html and reports for Journey Analytics.

		Hosts content for Rich Media feedback functionality, if enabled.
Google Inc.	USA	Optional data storage and processing of analytics data for Medallia for Digital Data storage and processing for Journey Analytics. Translates feedback text, if enabled in Customer's Medallia implementation.
AppDynamics, Inc.	USA	Analyzes performance and usage of survey pages and reporting applications.
Usersnap GmbH	Austria	Provides screen capture functionality, if enabled in Customer's Medallia Digital implementation.
Twilio	USA	Provides SMS routing and delivery services. Sendgrid is used to send emails to users in Journey Analytics.
Pendo.io	USA	Analyzes performance and usage of Strikedeck applications.
GFN DSelva Infotech Pvt Ltd	India	Performs development and quality assurance for Strikedeck applications.
Palo Alto Databases, Inc.	USA	Supports Strikedeck Enterprise's ETL tool.
Redis Labs Ltd.	USA	Redis for Caching service maintains state for cookies in Journey Analytics.

Medallia Subsidiaries

Medallia employees at its subsidiaries may access Customer's program instance to provide technical support, cloud operations, product troubleshooting, and infrastructure maintenance.

Subsidiary Name	**Location**
Medallia Canada, Inc.	Canada
Medallia S.A.	Argentina
Medallia Limited	United Kingdom
Medallia Australia PTY Ltd	Australia
Cooladata Ltd	Israel
Medallia Digital Ltd	Israel
Medallia GmbH	Germany

Annex B – 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 Experience Cloud;
- 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.

AMENDMENTS FOR DATA EXPORTERS LOCATED IN GERMANY

Rectification, deletion and blocking of data: Medallia shall rectify, delete and/or block Personal Data if so instructed by Customer.

Self-monitoring by Medallia: Medallia shall monitor, by appropriate means, its own compliance with its data protection obligations in connection with provision of the Medallia Experience Cloud.

Monitoring by the Data Exporter: Following the terms of section 5 of the DPA, Customer also have the right to carry out on-site audits during regular business hours, without disrupting Medallia's business operations and in accordance with Medallia's security policies, and after a reasonable prior notice. Medallia shall tolerate such audits and shall render all necessary support.

Notification obligation of Medallia: Medallia will notify Customer without undue delay of (i) any non-compliance with statutory provisions dealing with the protection of Personal Data by the Medallia or its employees, (ii) any non-compliance with the provisions of this Appendix 2. Medallia shall further notify Customer, without undue delay, if it holds that an instruction violates applicable laws. Upon providing such notification, Medallia shall not be obliged to follow the instruction, unless and until Customer has confirmed or changed it. Medallia shall notify Customer of data subjects' complaints and requests (e.g. regarding the rectification, deletion and blocking of data) and orders by courts and competent regulators and any other exposures or threats in relation to data protection compliance identified by Medallia.

Right to instruction: Customer is entitled and obliged to instruct Medallia in connection with provision of the Medallia Experience Cloud, generally or in the individual case, regarding the collection, processing and use of the data. Instructions may also relate to the correction, deletion or blocking of data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g. oral, electronic) form. Instructions in another form than in writing shall be confirmed by Customer in writing, if Medallia so requests.

Return and further use of data after end of contract: Upon the expiration or termination of this Appendix 2, unless otherwise instructed by the Customer, Medallia shall return to Customer, without undue delay, all data received from the Customer and all data obtained or generated in connection with provision of the Medallia Experience Cloud, and shall refrain from any further processing and use of such data, to the extent this is possible without infringing Medallia's own statutory obligations.

Data secrecy: Medallia shall be obliged to commit staff entrusted with the processing of Personal Data hereunder in written form to keeping any Personal Data strictly confidential and not to use such Personal Data for any other purposes except for the provision of the Medallia Experience Cloud to Customer. Medallia will further instruct its staff regarding the applicable statutory provisions on data protection.

Annex C - Model Clauses

Standard Contractual Clauses (processors)

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

'**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, 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;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

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 platform offered via a Software-as-a-Service model ("**Medallia Experience Cloud**") 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 B 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 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Underlying Agreements and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Underlying Agreements. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

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(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in section 5 (Security Reports and Audits) of this DPA.

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.