Data Processing Agreement

This Data Processing Agreement ("**DPA**") supplements and forms part of any master services agreement, applicable order form, or any other agreement ("**Agreement**") made between Demandbase, Inc. and its Affiliates ("**Demandbase**") and Customer regarding the Processing (defined below) of Personal Data (defined below), as part of the services provided by Demandbase to Customer under such Agreement ("**Services**"). This DPA shall only become legally binding between Customer and Demandbase when the instructions set out on the Knowledgebase page have been fully completed.

1. Definitions

Affiliate shall have the meaning set out in the Agreement.

Controller shall have the meaning set out in EU Privacy Law.

Controller to Processor SCCs means the Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of February 5, 2010, as may be amended or replaced from time-to-time by the European Commission.

Customer Data means Customer or Permitted Affiliates' Personal Data provided to Demandbase under the Agreement by Customer for which Demandbase is a data Processor.

Data Subject shall have the meaning set out in EU Privacy Law.

Data Subject Request means a request received from a Data Subject to exercise the right of access, rectification, restrict or object to Processing, erasure, data portability, or right not to be subject to automated decision-making.

EU Privacy Law means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**General Data Protection Regulation**" or "**GDPR**") and any other laws of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom applicable to the Processing of Personal Data under the Agreement.

Instruction means the written instructions issued by a Controller to Processor, as to perform a specific action with regards to Personal Data. For clarity, Instructions shall be specified in the Agreement, this DPA and, as otherwise amended, amplified or replaced by the Controller in writing (e.g., via email).

Permitted Affiliate means an Affiliate of Customer that is located in the European Economic Area that is permitted to use the Services under the Agreement but is not a Customer under the Agreement between Demandbase and Customer, has not signed its own Order Form with Demandbase and is not a "Customer" as defined under the Agreement.

Personal Data shall have the meaning set out in EU Privacy Law.

Principles means the Privacy Shield Framework principles of notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; and recourse, enforcement and liability; as well as any supplemental principles.

Privacy Shield means the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield framework as set forth by the US Department of Commerce.

Process or Processing shall have the meaning set out in EU Privacy Law.

Processor means any entity which Processes Personal Data on behalf of the Controller.

Security Documentation means Demandbase's security documentation available at https://support.demandbase.com/hc/en-us/articles/360000509903-Demandbase-Security-Practices, access to security audits (such as SOC 2) or other relevant information, as made available by Demandbase.

Security Incident means unlawful or accidental destruction, loss, alteration, unauthorized disclosure of, or access to the Customer Data, transmitted, stored, or otherwise processed by Demandbase or its Sub-processors of which Demandbase becomes aware.

Services has the meaning specified above.

Sub-processor means any legal person which Processes Customer Data on behalf of Demandbase, including any affiliate of Demandbase.

Supervisory Authority means an independent public authority which is established by an EU member state pursuant to the GDPR.

2. **Scope; Customer Responsibility**. Data Subjects affected by the Processing under this Agreement are those Data Subjects whose information is shared with Demandbase as Customer Data under the Agreement. For specific implementations of the Conversion solution, this Customer Data consists of CRM contact data of Customer's clients and prospects, Slack usernames, emails or other contact data for Customer's employees. For specific implementations of the Engagement solution, this Customer Data consists of email addresses of Customer's clients and prospects received from Customer's marketing automation system. Customer acknowledges and agrees that it has the sole responsibility for the lawfulness of the Processing of Personal Data on its behalf.

Customer represents and warrants that it is legally allowed to engage Demandbase for the Processing of Personal Data on Customer's behalf and has provided all necessary notices and obtained all required consents that meet the standard set forth in applicable law (including EU Privacy Law) from Data Subjects for the Processing described herein and in the Agreement. Customer shall be solely responsible for acting as the responsible body with regards to the transfer of Personal Data and for the accuracy, quality, and legality and the means by which Demandbase acquired the Personal Data.

3. Instructions and Exceptions.

a. **Instructions**. Customer's Instructions for the Processing of Customer Data shall comply with EU Privacy Law and any other applicable laws. Demandbase will only process Personal Data on Customer's behalf of and in accordance with Customer's Instructions. Customer instructs Demandbase to Process Customer Data: (a) in accordance with the Agreement and actions initiated by Customer's use of the Services; (b) pursuant to the features and limitations of the Services which Demandbase provides to Customer under the Agreement; and (c) for the providing and improving any Services requested for Customer.

b. **Exceptions**. Demandbase will be under no obligation to comply with Instructions that Demandbase deems as violating EU Privacy Law or other applicable laws. Processing outside of the scope of this DPA will require prior written agreement between Customer and Demandbase. In the event that Demandbase cannot comply with the instructions in section 3(a) (*Instructions*) then Demandbase will notify Customer and may terminate the Agreement or take any other reasonable action without liability.

4. Confidentiality. As required under article 28 of the GDPR, Demandbase will use commercially reasonable steps to ensure that its employees that are engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received training regarding their responsibilities, and are subject to a duty of confidentiality. Demandbase will ensure the reliability of its employees and that employees' access to Personal Data will be limited to those personnel performing the Services in accordance with the terms of the Agreement.

5. Security. Demandbase will take reasonable steps to maintain appropriate organizational and technical security measures for the protection of Customer Data; including, but not limited to, personnel, facilities, software, access controls, vulnerability management, to protect against the unauthorized or accidental loss, and unauthorized alteration, disclosure or destruction of Customer Data. Demandbase will take reasonable steps to confirm compliance with the foregoing measures, as required under this DPA and will not materially decrease the overall security of its Services during the term of this DPA. Upon receipt of a written request by Customer and subject to the confidentiality requirements in the Agreement, Demandbase may make available to Customer the Security Documentation and its most recent third party certifications or audit results, as applicable.

6. Sub-processors.

a. **Authorization.** Customer agrees that Demandbase may use Sub-processors, including its Affiliates, to carry out its obligations under the Agreement and herein. To the extent required under article 28 of the GDPR, Demandbase will (i) remain liable to Customer for the acts and omissions with regards to the Sub-processors as if performing the services of each Sub-processor directly under this DPA; and (ii) enter into contractual agreements with Sub-processors requiring them to provide the same level of protection as required herein. When applicable, this section also applies to the parties' obligations under section 11 of the Controller-to-Processor SCCs.

b. **Current List.** A list of current Sub-processors is available online at https://support.demandbase.com/hc/en-us/articles/360000384823-Demandbase-Sub-Processor-List and Customer agrees that Demandbase may provide prior notice by updating such list and any Sub-processors at the aforementioned link or via email update. If Customer requires prior notice via an email update, then Customer agrees to sign up through the aforementioned link and such update shall be effective as of the date the email is sent.

c. **Objections**. In the event that Customer objects to Demandbase's change of Sub-processors, Customer agrees to notify Demandbase promptly in writing, in any case with five (5) days of receiving notice of any updated Sub-processor list. In the event that Customer has a reasonable objection to a newly engaged Sub-processor, then Demandbase will either: (i) make reasonable efforts to make available to Customer a commercially-reasonable change to Customer's configuration; or (ii) recommend a change to avoid using the new Sub-processor or suggest another use of the Services to avoid using the objected to new Sub-processor. If Demandbase is unable to make available such a change within a reasonable amount of time (which shall be at least 60 days), then Customer may terminate the applicable Order Form by providing written notice to Demandbase with respect to only those aspects of the Service that cannot be provided without the use of the objected-to new Sub-processor.

d. **Copies**. In the event that Customer is required to share copies of Demandbase Sub-processor agreements under EU Privacy Law or, if applicable, under section 5(j) of the Controller-to-Processor SCCs, then Demandbase may remove any commercial terms or their equivalent before providing the agreements and that such copies will be provided by Demandbase, in its discretion, only upon written request by Customer.

7. Data Subject Requests. In the event that Demandbase receives a valid Data Subject Request, Demandbase will promptly notify Customer of the Data Subject Request, provided that it is legally permissible to do so. Demandbase will not respond to such request except to confirm that it corresponds to Customer. Taking into account the nature of the Processing and to the extent legally permitted, Demandbase will provide commercially reasonable assistance to Customer, using appropriate organizational and technical measures to assist Customer with fulfilling its obligation to respond to Data Subject Requests under EU Privacy Law to the extent that Customer does not otherwise have the ability to respond to the Data Subject Request through its use of the Services. When legally permitted, Customer will be responsible for any costs related to Demandbase's provision of such services.

8. Data Protection Officer. Demandbase has appointed a data protection officer effective May 25, 2018. Customer may reach such data protection officer at dpo@demandbase.com.

9. Incident Management and Customer Security Obligations. Demandbase has reasonable and appropriate security incident management policies and procedures and will notify Customer without undue delay after becoming aware of a Security

Incident as it relates to Customer Data. Demandbase will reasonably assist Customer to the extent required by Demandbase under EU Privacy Law with regards to Customer's obligation to notify the Supervisory Authority. Demandbase will make reasonable efforts to identify the cause of the Security Incident. To the extent that remediation is under Demandbase's reasonable control, Demandbase will take steps that it deems necessary and reasonable to remediate the cause of the Security Incident and share with Customer any related information required to be shared under EU Privacy Law. The obligations herein do not apply to any Security Incidents that are caused by Customer or Customer's users or to unsuccessful attempts of Security Incidents. Demandbase will notify Customer of any Security Incidents to the primary account holder's email address listed within Demandbase's systems. Customer acknowledges that it is solely responsible for ensuring that its contact information is up-to-date. Demandbase's response to or notification of a Security Incident will not be construed as an acknowledgement by Demandbase of any fault or liability with respect to the Security Incident. Customer is solely responsible for: (i) securing its account, authentication credentials, and any systems or devices that Customer uses to access the Services and (ii) backing up any Customer Data. Demandbase has no obligation to protect Customer Data that Customer elects to store outside of Demandbase and its Sub-processors' systems, such as those Customer elects to share with Third Party Applications (as defined in the Agreement). Customer acknowledges that it is solely responsible for reviewing the Security Documentation and evaluating the Services. Customer agrees that taking into the state of the art, costs, account the nature, scope, context, and purposes of Processing of the Customer Personal Data and the risks to individuals, the security measures implemented by Demandbase as set out in section 5 (*Security*) provide a level of security appropriate to the risk in respect of the Customer Data. In the event that Customer suspects that a potential Security Incident has occurred, Customer agrees to immediately contact Demandbase as specified in its Customer Security Incident Reporting Process.

10. Data Protection Impact Assessment. Demandbase makes available documentation through its Knowledgebase, which facilitates Customer's compliance with the obligation under EU Privacy Law to carry out a data protection impact assessment. Upon Customer's written request, Demandbase will provide Customer with reasonable assistance, at Customer's expense to the extent permitted under law, to fulfill Customer's obligation under EU Privacy Law to carry out a data protection impact assessment related to Customer's use of the Service. Demandbase will provide such assistance to the extent that: (i) it has access to the relevant information; and (ii) that Customer does not otherwise have access to the relevant information. Demandbase will provide reasonable assistance to Customer to cooperate with the Supervisory Authority to the extent required under EU Privacy Law.

11. Audits. No more than once per year, solely for the purpose of meeting its audit requirements under Article 28, section 3(h) of the GDPR or, if applicable, its obligations under 5(f) and 12(2) of the Controller-to-Processor SCCs, Customer may request an audit in writing. Customer agrees to exercise the aforementioned audits by instructing Demandbase to conduct a System and Organization Controls (SOC) 2 Audit at Demandbase's expense. Subject to the confidentiality terms in the Agreement, Demandbase will make available to Customer any reasonably necessary information that demonstrates Demandbase's compliance with the its obligations in this DPA or the Controller-to-Processor SCCs in the form of Such SOC 2 Report and any third party certifications and audits.

12. Data Transfers.

a. **Privacy Shield.** The parties hereby agree and confirm that when Demandbase is certified under the Privacy Shield framework to receive Personal Data from the European Economic Area ("**EEA**"), then Demandbase may choose to rely on its Privacy Shield certification. In the event that Demandbase chooses to rely on its Privacy Shield Certification, the parties agree that Demandbase will: (i) use the Personal Data for the purposes permitted in the Agreement through the instructions of Customer; (ii) provide appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or loss, alternation, unauthorized disclosure or access, and understands whether onward transfer is allowed; (iii) taking into account the nature of the processing, assist Customer in responding to individuals exercising their rights under the Principles; (iv) comply with the Privacy Shield Principles when Processing Personal Data from the EEA; (v) to the extent that Demandbase engages a third party to process EEA Personal Data, Demandbase shall take reasonable and appropriate steps to: (a) ensure that such third party provides at least the same level of protection for EEA Personal Data as required by the Privacy Shield Principles and (b) stop and remediate unauthorized processing, upon notice; and (vi) authorizes Customer to provide these Privacy Shield clauses and a copy of any relevant privacy provisions under the Agreement to the Department of Commerce upon its request (as required under the Accountability for Onward Transfer Principle of the Privacy Shield). In the aforementioned sentence, (i), (ii), (iii), (iv), and (v) shall survive termination of these clauses and the Agreement for so long as Demandbase has custody, control, or possession of the Personal Data; and (vi) shall survive indefinitely.

In the event that Privacy Shield is invalidated as an adequate transfer mechanism or Demandbase is no longer certified, then the Controller-to-Processor SCCs apply and are incorporated herein by reference. The terms in this DPA set out the parties' interpretation of their respective obligations under the specific clauses of the Controller-to-Processor SCCs identified herein. As permitted by Clause 10 of the Controller-to-Processor SCCs, the purpose of the interpretations is to enable the parties to fulfil their obligations in practice. Where a party complies with the interpretations set out in this DPA, that party shall be deemed by the other party to have complied with its commitments under the Controller-to-Processor SCCs. In the event that there is a conflict between the terms herein and the Controller-to-Processor SCCs, the terms in the Controller-to-Processor SCCs shall prevail.

13. Return and Deletion of Data. Demandbase will delete or return Customer Data to Customer upon the termination of the Agreement and will delete any copies unless otherwise required under applicable law. Demandbase will only provide certification of deletion upon receipt of a written request by Customer for its obligations herein and, if applicable, as required under section 12(1) of the Controller-to-Processor SCCs. Any requests to return Customer Data must be made within 60 days after the termination of the Agreement.

14. Liability. Demandbase and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA and all data processing agreements between Customer, Permitted Affiliates and Demandbase, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all data processing agreements together. Demandbase and its Affiliates' total liability for all claims from Customer and all Permitted Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all data processing agreements established under this DPA or the Agreement, including by Customer and all Permitted Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Permitted Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its appendices, attachments, or terms incorporated by reference.

15. Permitted Affiliates. When a Permitted Affiliate becomes a party to the DPA, then such Permitted Affiliate shall be entitled to exercise its rights and remedies available under this DPA to the extent required under applicable EU Privacy Law. However, if applicable EU Privacy Law requires the Permitted Affiliate to directly exercise a right or remedy against Demandbase directly by itself, the parties agree that to the extent permitted under law: (i) only the Customer that is the contracting entity to the Agreement shall exercise any such right or seek any such remedy on behalf of the Permitted Affiliate; and (ii) the Customer that is the contracting entity to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Permitted Affiliates together, instead of doing so separately for each Permitted Affiliate. The Customer that is the contracting entity is responsible for coordinating all communication with Demandbase under the DPA and be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

16. Third Party Controllers. If EU Privacy Law applies to the Processing of Customer Personal Data and Customer is a Processor, then Customer warrants to Demandbase that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Demandbase as another Processor, have been authorized by the relevant Controller.

17. Applicability. This DPA is incorporated into and forms part of the Agreement. Except as expressly set forth in this DPA, the terms and conditions of the Agreement shall remain in full force and effect. In the event of a conflict between this DPA and the Agreement, the terms of this DPA take precedence unless any EU Privacy Law or any other legal or statutory requirements require that the terms of the Agreement to take precedence. For clarity, this DPA applies to Demandbase's processing of Personal Data as a Processor, not as an independent Controller.

IN WITNESS WHEREOF, the Parties have executed this Agreement by their duly authorized representative as of the date set forth below.

Demandbase, Inc.	**Customer:**
Signature: Fatima Khan	**Signature:**
Name: Fatima Khan	**Name:**
Title: Sr. Director, Legal & Chief Privacy Officer	**Title:**
Date: January 16, 2019 | 4:15 PM PST	**Date:**