DATA PROCESSING ADDENDUM TO THE UNIFIED PILOT RESEARCH AGREEMENT
(GDPR and Standard Contractual Clauses)
(July 2019)

This Data Processing Addendum to the Unified Pilot Research Agreement, including its Schedules and Appendices, ("Pilot DPA") forms part of the Unified Pilot Research Agreement ("Pilot Agreement") between SFDC and Customer to which it is attached, to reflect the parties’ agreement with regard to the Processing of Personal Data submitted to the Covered Services. For the avoidance of doubt, this Pilot DPA does not apply to any GA Services as defined in the Pilot Agreement.

By signing the Pilot Agreement, Customer enters into this Pilot DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent SFDC processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this Pilot DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Pilot Agreement.

In the course of providing the Covered Services to Customer pursuant to the Pilot Agreement, SFDC may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorized Affiliate” means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Covered Services pursuant to the Pilot Agreement between Customer and SFDC, but is not a "Customer" as defined under the Pilot Agreement.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations 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 Pilot Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“Data Science Programs” means those projects undertaken by SFDC, in which Customer shall allow SFDC to access and use Customer Data, for the purposes of (i) building, analyzing, reviewing, running, training testing and improving algorithms and machine learning models to be used in GA Successor and Non-GA Services and (ii) performing analyses on the Customer Data.


“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.
“Pilot Term” means what is defined as “Term” in accordance with Section 9 of the Pilot Agreement.

“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.

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

“SFDC Group” means SFDC and its Affiliates engaged in the Processing of Personal Data.

“Standard Contractual Clauses” means the agreement executed by and between Customer and salesforce.com, inc. and attached hereto as Schedule 2 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

“Sub-processor” means any Processor engaged by SFDC or a member of the SFDC Group.

“Supervisory Authority” means any independent public authority which is established by an EU Member State pursuant to the GDPR.

2. **PROCESSING OF PERSONAL DATA**

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, SFDC is the Processor and that SFDC or members of the SFDC Group will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2 **Customer’s Processing of Personal Data.** Customer shall, in its use of the Covered Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 **Sensitive Data.** The following types of sensitive Personal Data (including images, sounds or other information containing or revealing such sensitive data) may not be submitted to the Covered Services: government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, information concerning health or sex life; information related to an individual’s physical or mental health; and information related to the provision or payment of health care.

2.4 **SFDC’s Processing of Personal Data.** SFDC shall treat Personal Data as confidential and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Pilot Agreement; (ii) Processing initiated by Users in their use of the Covered Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Pilot Agreement; and (iv) Processing to train and improve the Covered Services and any other of SFDC’s current and future features, products and/or services.

2.5 **Details of the Processing.** The subject-matter of Processing of Personal Data by SFDC is the performance of the Covered Services pursuant to the Pilot Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this Pilot DPA are further specified in Schedule 1 (Details of the Processing) to this Pilot DPA.

3. **RIGHTS OF DATA SUBJECTS**

3.1 **Data Subject Request.** SFDC shall, to the extent legally permitted, promptly notify Customer if SFDC receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a “Data Subject Request”. Taking into account the nature of the Processing, SFDC shall assist Customer by appropriate
technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Covered Services, does not have the ability to address a Data Subject Request, SFDC shall upon Customer’s request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SFDC is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from SFDC’s provision of such assistance.

4. **SFDC PERSONNEL**

4.1 **Confidentiality.** SFDC shall ensure that its 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. SFDC shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Reliability.** SFDC shall take commercially reasonable steps to ensure the reliability of any SFDC personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** SFDC shall ensure that SFDC’s access to Personal Data is limited to those personnel performing Covered Services in accordance with the Pilot Agreement.

4.4 **Data Protection Officer.** Members of the SFDC Group have appointed a data protection officer. The appointed person may be reached at privacy@salesforce.com.

5. **SUB-PROCESSORS**

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) SFDC’s Affiliates may be retained as Sub-processors; and (b) SFDC and SFDC’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Covered Services. SFDC or a SFDC Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Pilot DPA and Pilot Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Processing provided by such Sub-processor.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.** SFDC shall make available to Customer the current list of Sub-processors for the Covered Services identified in Appendix 3 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location (“Infrastructure and Sub-processor Documentation”). Customer may find on SFDC’s Trust and Compliance webpage (also accessible via http://www.salesforce.com/company/legal/agreements.jsp under the “Trust and Compliance Documentation” link) the Infrastructure and Sub-processor Documentation as well as a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, SFDC shall provide notification to Customer of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Covered Services.

5.3 **Objection Right for New Sub-processors.** Customer may object to SFDC’s use of a new Sub-processor by notifying SFDC promptly in writing within ten (10) business days after receipt of SFDC’s notice made in accordance with Section 5.2. In the event Customer objects to a new Sub-processor for the Covered Services, as permitted in the preceding sentence, Customer’s sole remedy is to terminate the Pilot Agreement and cease use of the Covered Services.

5.4 **Liability.** SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this Pilot DPA, except as otherwise set forth in the Pilot Agreement.

6. **SECURITY AND PRIVACY CONTROLS**

6.1 **Controls for the Protection of Customer Data.** SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and
against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Measures for the Covered Services are set forth in the Security, Privacy and Architecture Documentation found at https://www.salesforce.com/company/legal/agreements as updated from time to time.

6.2 Audits. With respect to the Covered Services, to the extent required by applicable Data Protection Laws and Regulations and not covered by the applicable GA Service(s) Documentation, upon Customer’s request, SFDC shall make available to Customer information necessary to demonstrate compliance with such applicable Data Protection Laws and Regulations. Only to the extent that the provision of information or documents as referred to in this Section does not satisfy the Customer’s obligations under applicable Data Protection Laws, and only to the extent SFDC is required to make available to Customer an on-site audit right by applicable Data Protection Laws and Regulations, Customer may request information related to a Covered Service when it conducts an on-site audit of the applicable GA Service under the customer’s Master Subscription Agreement with SFDC.

6.3 Data Protection Impact Assessment. To the extent required by applicable Data Protection Laws and Regulations, upon Customer’s request, SFDC shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer’s obligation under such Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer’s use of the Covered Services, to the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to SFDC. SFDC shall provide reasonable assistance to Customer in the cooperation or prior consultation with an applicable Supervisory Authority in the performance of its tasks relating to this Section of the Pilot DPA, to the extent required by applicable Data Protection Laws and Regulations.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

SFDC maintains security incident management policies and procedures as specified in the Security, Privacy and Architecture Documentation for the applicable GA Service associated with the Covered Services and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by SFDC or its Sub-processors of which SFDC becomes aware (a “Customer Data Incident”). SFDC shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as SFDC deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within SFDC’s reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer’s Users.

8. RETURN AND DELETION OF CUSTOMER DATA

When Customer’s right to use a Non-GA Service ends, if Customer continues using a Covered Service as a GA Service, SFDC’s return and deletion of Personal Data processed by the Covered Services shall be in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation for the related GA Service. If Customer does not continue to use the Covered Service as a GA Service, Customer may export or request return of its data for 30 days after Customer’s right to use the Non-GA Service ends, after which Customer Data shall be subject to deletion.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Pilot Agreement, the Customer enters into the Pilot DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between SFDC and each such Authorized Affiliate subject to the provisions of the Pilot Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this Pilot DPA and, to the extent applicable, the Pilot Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Pilot Agreement, and is only a party to the Pilot DPA. All access to and use of the Covered Services and Content by Authorized Affiliates must comply with the terms and conditions of the Pilot Agreement and any violation of the terms and conditions of the Pilot Agreement by an Authorized Affiliate shall be deemed a violation by Customer.
9.2 Communication. The Customer that is the contracting party to the Pilot Agreement shall remain responsible for coordinating all communication with SFDC under this Pilot DPA and be entitled to make and receive any communication in relation to this Pilot DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the Pilot DPA with SFDC, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this Pilot DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this Pilot DPA against SFDC directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Pilot Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Pilot Agreement shall exercise any such rights under this Pilot DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Pilot Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on SFDC and its Sub-Processors by combining, to the extent possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

SFDC’s and all of its Affiliates’ liability under this DPA shall be subject to the “No Damages” section of the Pilot Agreement, to the maximum extent permitted under applicable Data Protection Laws and Regulations. If the “No Damages” section is deemed impermissible, SFDC’s and all of its Affiliates’ liability under this DPA shall be capped at $10,000.

11. TRANSFER MECHANISMS FOR DATA TRANSFERS TO THIRD COUNTRIES

11.1 Transfer Mechanisms for European Data Transfers. To the extent that Customer’s use of the Covered Services under the Pilot Agreement involves the transfer of Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws and Regulations of the foregoing territories, the Standard Contractual Clauses attached as Schedule 2 to this Pilot DPA shall apply, whereby Customer and its Authorized Affiliates shall be the “data exporter(s)” and SFDC and SFDC’s Affiliates shall be the “data importer(s).”

11.2 Additional Terms for Standard Contractual Clauses.

11.2.1 Instructions. This Pilot DPA and the Pilot Agreement are Customer’s complete and final documented instructions at the time of signature of the Pilot Agreement to SFDC for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to Process Personal Data: (a) Processing in accordance with the Pilot Agreement; (b) Processing initiated by Users in their use of the Covered Services; and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Pilot Agreement.

11.2.2 List of Current Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) SFDC’s Affiliates may be retained as Sub-processors; and (b) SFDC and SFDC’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Covered Services. SFDC shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA.
11.2.3 **Notification of New Sub-processors and Objection Right for New Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that SFDC may engage new Sub-processors as described in Sections 5.2 of the Pilot DPA and that Customer may object to SFDC’s use of a new Sub-processor in accordance with Section 5.1 of the Pilot DPA.

11.2.4 **Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by SFDC to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent removed by SFDC beforehand; and, that such copies will be provided by SFDC, in a manner to be determined in its discretion, only upon request by Customer.

11.2.5 **Audits.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section 6.2 of the Pilot DPA.

11.2.6 **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by SFDC to Customer only upon Customer’s request.

11.2.7 **Conflict.** In the event of any conflict or inconsistency between the body of this Pilot DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 5, with respect to Personal Data that relates to European Data Subjects, the Standard Contractual Clauses shall prevail.

**List of Schedules**

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses
SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

SFDC will Process Personal Data as necessary to perform the Covered Services pursuant to the Pilot Agreement and Pilot DPA, as further specified in the Documentation, and as further instructed by Customer in its use of the Covered Services.

Duration of Processing

Return and deletion of Personal Data will take place in accordance with Section 8 of the Pilot DPA.

Categories of Data Subjects

Customer may submit Personal Data to the Covered Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer’s prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer’s Users authorized by Customer to use the Covered Services

Type of Personal Data

Customer may submit Personal Data to the Covered Services, 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 categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data
SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address: 
Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

(the data exporter)

And

Name of the data importing organisation: salesforce.com, inc.

Address: 415 Mission Street, Third Floor, San Francisco, CA 94105, USA
Tel.: + 1 415 901 7000; fax: + 1 415 901 7400; e-mail: privacy@salesforce.com

Other information needed to identify the organisation: Not applicable

(the data importer)

each a “party”; together “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.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '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;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) '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;

(d) '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;

(e) '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;

(f) '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.

Clause 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.

Clause 3

Third-party beneficiary clause

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.

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. 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.

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.

Clause 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;
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).

**Clause 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 subprocession, 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 subprocession, 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.

Clause 6

Liability

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.

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.

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

3. 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.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

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.

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).

Clause 9

Governing Law

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

Clause 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.

Clause 11

Subprocessing

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.

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.

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.

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.

Clause 12

Obligation after the termination of personal data processing services
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.

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.

On behalf of the data exporter:

Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature:

_____________________
(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Jenna Hillard
Position: Sr. Manager, Order Management
Address: salesforce.com, inc., 415 Mission St. Third Floor, San Francisco, CA 94105, United States
Other information necessary in order for the contract to be binding (if any): Not applicable

Signature:

_____________________
(stamp of organisation)
APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Authorized Affiliates (as defined in the Pilot DPA) of Customer established within the European Economic Area (EEA), Switzerland, and UK that have purchased Covered Services under the Pilot Agreement.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Salesforce.com, inc. is a provider of enterprise cloud computing solutions which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the Pilot Agreement and Pilot DPA.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter’s prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter’s Users authorized by data exporter to use the SCC Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data
Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
Data exporter may submit special categories of data to the Covered Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Covered Services pursuant to the Pilot Agreement.

DATA EXPORTER

Name:

Authorised Signature: __________________________

DATA IMPORTER

Name: Jenna Hillard

Authorised Signature: __________________________
APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses and must be completed and signed 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):

Data importer shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data. Measures for the applicable GA Service(s) associated with the Covered Services are set forth in the Security, Privacy and Architecture Documentation for the applicable GA Service(s), and may apply depending upon the Covered Services in question.

DATA EXPORTER
Name:

Authorised Signature:____________

DATA IMPORTER
Name: Jenna Hillard

Authorised Signature:
APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

- Salesforce Services (services branded as Force.com, Site.com, Database.com, Sales Cloud, Service Cloud, Community Cloud and Chatter) as well as Financial Services Cloud, Health Cloud, Salesforce Quote-to-Cash, Work.com and all Einstein-branded features of the foregoing services.
- Advertising Studio (formerly branded as Social.com and Active Audiences)
- B2B Commerce (formerly branded as CloudCraze)
- Commerce Cloud (formerly branded as Demandware)
- Data.com
- Datorama
- Desk.com
- Einstein Analytics (formerly branded as Analytics Cloud or Wave Analytics)
- Einstein Discovery (formerly branded as BeyondCore)
- Einstein Vision and Language
- ExactTarget
- Heroku
- Interaction Studio
- IoT Cloud
- LiveMessage
- MuleSoft
- Pardot
- Predictive Intelligence
- Quip
- SalesforceIQ CRM
- Salesforce DMP (formerly branded as Krux) and Salesforce Data Studio
- Salesforce Inbox (including services branded as Salesforce Inbox)
- Social Studio