This Vendor Controller to Controller Privacy Exhibit ("C2C Vendor Privacy Exhibit") is entered between you ("Supplier") and salesforce.com, inc., a Delaware corporation, and its Affiliates ("SFDC") and forms part of the Agreement (as defined below) between SFDC and Supplier (the "Agreement"). This C2C Vendor Privacy Exhibit is effective as of the effective date of the Agreement (the "Effective Date") and shall remain in force unless and until terminated in accordance with the Agreement. All capitalized terms that are not expressly defined in this C2C Vendor Privacy Exhibit will have the meanings given to them in the Agreement.

1. Definitions

1.1 The definitions of “Controller”, “Personal Data”, “Processing”, “Data Subject”, “Supervisory Authority” and “Personal Data Breach” are as defined under the GDPR.

1.2 “Agreement” means any and all agreements and contracts relating to data Processing between SFDC and Supplier.

1.3 “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.

1.4 “Data Protection Laws” means all laws, regulations, and legally binding requirements of any governmental authority or regulator applicable to the Processing of Personal Data under the Agreement. This includes laws and regulations of the United States, the European Union, the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, including but not limited to GDPR.

1.5 “GDPR” means General Data Protection 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, and repealing Directive 95/46/EC.

2. Roles of the Parties; Details of the Processing. The parties acknowledge and agree that Supplier may receive Personal Data from SFDC and/or its Affiliates in their role as Controllers of that Personal Data, in order to fulfill its obligations under the Agreement. Within the scope of that Agreement, Supplier will Process the Personal Data in the role of a Controller of that Personal Data, whilst SFDC and/or its Affiliates remain separate Controllers of that Personal Data. Supplier agrees to Process the Personal Data received from SFDC solely for the purpose for which it has received the Personal Data under the Agreement, as specified in Annex B to Schedule 1, and in accordance with applicable Data Protection Laws.

3. Compliance with Data Protection Laws. Supplier will Process any Personal Data it receives from SFDC in accordance with the provisions of this C2C Vendor Privacy Exhibit and in accordance with Data Protection Laws. Supplier will promptly notify SFDC and co-operate with SFDC if it believes that it may no longer be able to comply with any of the terms of this C2C Vendor Privacy Exhibit or with Data Protection Laws.

4. Cooperation between the Parties. Supplier will assist SFDC to comply with requests or complaints of Data Subjects or Supervisory Authorities regarding compliance with Data Protection Laws with regard to Personal Data disclosed to Supplier. Supplier will notify SFDC of any requests, enquiries, monitoring activities and similar measures undertaken by Supervisory Authorities regarding the Processing under this C2C Vendor Privacy Exhibit.
5. Technical and Organizational Measures. Supplier shall implement appropriate technical and organizational measures to ensure an adequate protection of the Personal Data in accordance with its obligations under the GDPR. The receiving Party will regularly test, assess and evaluate the effectiveness of these measures.

6. Personal Data Breach Notification. Supplier shall notify SFDC without undue delay in the event a Personal Data Breach occurs that Supplier will notify to the competent supervisory authority or other regulator and/or the impacted Data Subjects.

7. Rights of Data Subjects. Notwithstanding Section 8 of this C2C Vendor Privacy Exhibit, the parties are, in their roles as separate Controllers, individually responsible for fulfilling the rights of Data Subjects regarding the Processing of Personal Data transferred under this C2C Vendor Privacy Exhibit.

8. Employee Personal Data. The parties agree to take all necessary measures to ensure that SFDC’s or its Affiliates' employees can exercise their rights under the GDPR with respect to the Personal Data that Supplier has received under the Agreement. For this purpose, and in addition to any rights SFDC’s or its Affiliates' employees may have pertaining to the Processing of their Personal Data by Supplier or SFDC or its Affiliates under this C2C Vendor Privacy Exhibit, the C2C Transfer Clauses or applicable Data Protection Laws, the parties agree that Supplier shall provide all necessary assistance required and shall not impede the fulfillment of these obligations. For the purposes of this Section 8, the term “employees” shall include temporary contractors and others in similar relevant relationships with SFDC or its Affiliates.

9. Incorporation of C2C Transfer Clauses. The parties agree that the Controller to Controller Standard Contractual Clauses approved by EC Commission Decision of 27 December 2004 (C(2004)5721) in Schedule 1 (“C2C Transfer Clauses”) will apply in addition to the provisions in this C2C Privacy Vendor Exhibit. The C2C Transfer Clauses shall be incorporated into this C2C Privacy Vendor Exhibit by reference and shall be considered duly executed between the parties upon entering into force of this C2C Privacy Vendor Exhibit. For the avoidance of doubt, the C2C Transfer Clauses shall apply to the transfer of Personal Data from any SFDC Affiliate based in the EEA and their member states, Switzerland and the United Kingdom to Supplier or any of its Affiliates that are based in a third-country that is not deemed to be adequate by the European Commission.

10. Identity of Data Exporter. SFDC signs the C2C Transfer Clauses in name and on behalf of its Affiliates that qualify as data exporter and that are based in the European Union.

11. Conflicts. In the event of any conflict between the data protection terms in the Agreement and this C2C Vendor Privacy Exhibit, the relevant terms of the C2C Privacy Exhibit will take precedence. In the event of any conflict between the provisions of the C2C Transfer Clauses and the remaining terms of this C2C Vendor Privacy Exhibit, the C2C Transfer Clauses shall take precedence. The parties’ authorized signatories have duly executed this C2C Vendor Privacy Exhibit, including the C2C Transfer Clauses, as of the Effective Date.

12. Successor Mechanisms for C2C Transfer Clauses. In the event that the C2C Transfer Clauses are amended, replaced or repealed by the European Commission or otherwise under Data Protection Laws, the parties shall work together in good faith to enter into any updated version of the C2C Transfer Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws. SFDC may terminate this C2C Vendor Privacy Exhibit and the Agreement on 30 days’ written notice, if the parties are incapable of implementing or fail to implement another appropriate safeguard to ensure an adequate level of data protection within a period of 90 days.
SCHEDULE 1 – STANDARD CONTRACTUAL CLAUSES

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement between
salesforce.com, inc,
Salesforce Tower
415 Mission Street, 3rd Floor
San Francisco, CA 94105 USA
Tel.: + 1 415 901 7000; fax: + 1 415 901 7400; e-mail: privacy@salesforce.com

hereinafter “data exporter”

and

Contact information related to the data importer found in the Agreement

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

(a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) “the data exporter” shall mean the controller who transfers the personal data;

(c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references
to them (where relevant, and not including legal advice) of the country in which the data exporter is established.  

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.  

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.  

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.  

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.  

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfill the undertakings set out in these clauses.  

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).  

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).  

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.  

(h) It will process the personal data in accordance with the data protection laws of the country in which the data exporter is established.  

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

   (i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or
(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

II. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the “indemnified party(ies)”) promptly notifying the other party(ies) (the “indemnifying party(ies)”) of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.

(c) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

(d) Each party shall perform its obligations under these clauses at its own cost.

III. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

IV. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter’s country of establishment or of the authority which is final and against which no further appeal is possible.

V. Termination
In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);
(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
(iv) a final decision against which no further appeal is possible of a competent court of the data exporter’s country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VI. Variation of these clauses
The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VII. Description of the Transfer
The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.
ANNEX A
DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.
ANNEX B
DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred may include 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

Purposes of the transfer(s)
The transfer is made for the following purposes:

Performance of the services provided by data importer to data exporter in accordance with the Agreement.

Categories of data
The personal data transferred may include the following categories of 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
- Localisation data

Recipients
The personal data transferred may only be disclosed to the following recipients or categories of recipients:

Processing of personal data is limited to those personnel performing services in accordance with the Agreement.

Sensitive data (if appropriate)
The personal data transferred concerns the following categories of sensitive data:

Data exporter may transfer special categories of data to the data importer, and which is for the sake of clarity is 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 purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data protection registration information of data exporter (where applicable)

Not applicable

Additional useful information (storage limits and other relevant information)

As set forth in the Agreement.
Contact points for data protection enquiries

Data importer Contact points for Data importer can be found in the Agreement.

Data exporter: Email: privacy@salesforce.com, Tel.: +1 415 901 7000; fax: +1 415 901 7400