SALESFORCE VENDOR PRIVACY EXHIBIT

This Vendor Privacy Exhibit ("**Vendor Privacy Exhibit**") is entered into between salesforce.com, inc. ("**SFDC**") and supplier ("**Supplier**") as of the Effective Date set forth the Vendor Privacy Amendment and forms part of the Agreement (as defined below) between SFDC and Supplier. All capitalized terms that are not expressly defined in this Vendor Privacy Exhibit will have the meanings given to them in the Agreement. In case of a conflict between the terms of this Vendor Privacy Exhibit and the Agreement, this Vendor Privacy Exhibit will control. All examples are illustrative and not the sole examples of a particular concept.

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.

"Agreement" means the Agreement entered into between SFDC and Supplier for the provision of Supplier's Services to SFDC.

"Confidential Information" has the meaning as set forth in the Agreement.

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

"SFDC Customer Data" means (a) data or information submitted by or for SFDC Customers to SFDC's online services (including services of SFDC Affiliates) and (b) all data or information disclosed by or for SFDC Customers to SFDC in connection with receiving services from SFDC, including payment information. Customer Data may include Personal Data.

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

"Data Subject" means the individual to whom Personal Data relates.

"Data Protection Laws and Regulations" 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 and their member states, Switzerland and the United Kingdom, including but not limited to GDPR.

"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.

"Personal Data" means any information relating to an identified or identifiable natural person (the Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Protected Information" means (a) SFDC Customer Data and (b) all Personal Data that SFDC may provide to Supplier, including Personal Data about (i) SFDC prospective customers, suppliers and other business partners (and their respective employees and personnel) and (ii) Personal Data about SFDC employees and personnel.

"Security Breach" means (i) the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Protected Information or Confidential Information transmitted, stored or otherwise processed by Supplier or its Sub-processors or (ii) an event which led Supplier to suspect or would lead a reasonable person exercising a reasonable level of diligence and investigation to suspect that (i) has occurred.

"Services" means any goods and/or services that Supplier provides to SFDC under the Agreement.

"SFDC" means salesforce.com, inc., a company incorporated in Delaware.

"SFDC Customer" means a customer who purchases services from SFDC.

"Sub-processor" means an entity which Processes Protected Information on behalf of Supplier, who is a Processor of Protected Information on behalf of the Controller.

2. PRIVACY REQUIREMENTS

2.1 Compliance with Applicable Laws. With respect to its activities hereunder involving Protected Information, Supplier hereby represents, warrants and covenants that: (i) it is and will remain at all times during the term of this Agreement, and to the extent it Processes any Protected Information after the term of the Agreement, in compliance with all applicable Data Protection Laws and Regulations and will enable SFDC to use the Services in compliance with all Data Protection Laws and Regulations applicable to SFDC and the customers to whom SFDC provides services; and (ii) its performance under this Agreement will not cause SFDC to be in violation of any Data Protection Laws and Regulations.

2.2 **Written Instructions on Processing of Protected Information**. Supplier shall Process Protected Information only on behalf of and in accordance with SFDC's documented written instructions. If any other Processing is required by applicable Data Protection Laws and Regulations, Supplier shall inform SFDC of the legal requirement before commencing such Processing, unless providing this information to SFDC is legally prohibited. For purposes of this section, SFDC instructs Supplier to Process Protected Information for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s) and/or Statement(s) of Work and (ii) Processing to comply with other documented reasonable instructions provided by SFDC (e.g., via email) where such instructions are consistent with the terms of the Agreement. Further details on the Supplier's Processing activities under this Agreement are set out in Schedule 1. Supplier shall immediately inform SFDC if, in its opinion, an instruction from SFDC infringes Data Protection Laws and Regulations.

2.3 **Provision of Information to Demonstrate Compliance**. Supplier shall make available to SFDC all information necessary to demonstrate Supplier's compliance with the obligations laid down in this Vendor Privacy Exhibit.

2.4 **Personnel and Third Parties Authorized to Process Protected Information**. Supplier shall treat Protected Information as Confidential Information and shall not disclose Protected Information to any of its personnel or any third party except as necessary to perform the Services. Supplier shall ensure that personnel or third parties authorized to Process the Protected Information: (i) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, (ii) are informed of the confidential nature of the Protected Information, (iii) have received appropriate training on their responsibilities and (iv) do not Process Protected Information except on written instructions from SFDC, unless required by applicable law.

2.5 **Technical and Organizational Measures**. Supplier shall implement and maintain appropriate technical and organizational measures (and provide reasonable assistance to SFDC in implementing its own technical and organizational measures to the extent SFDC's implementation of such measures are dependent on Supplier) in order to:

a. Protect Protected Information and Confidential Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or Processing in accordance with Data Protection Laws and Regulations, thereby taking into account the principles of privacy-by-design and privacy-by-default.
b. Enable SFDC to meet its legal obligations to respond to requests from individuals under Data Protection Laws and Regulations in a timely manner, including the ability of Supplier to implement requests from individuals to access, rectify, amend, object to Processing, erase, not to be subject to automated decision-making including profiling, or port their Personal Data or to restrict or cease Processing of such Personal Data where SFDC instructs Supplier to implement such a request. Supplier shall immediately notify SFDC of any request related to SFDC made by an individual to exercise any individual right under Data Protection Laws and Regulations and shall cooperate with SFDC in executing SFDC's obligations related to such request. Supplier may not reach out to the individual without SFDC's prior written consent except to confirm that the request relates to Salesforce.
c. Ensure and be able to demonstrate that Processing of Protected Information is performed in accordance with applicable Data Protection Laws and Regulations.

2.6 **Data Protection Impact Assessment**. Upon SFDC's request, Supplier shall assist SFDC when SFDC carries out any data protection impact assessment related to Processing carried out with respect to Supplier's Services under the Agreement and provide assistance to SFDC in SFDC's consultation with regulators regarding the Processing that is the subject of a data protection impact assessment. If Supplier Processes SFDC Customer Data, upon SFDC's request, Supplier shall also provide SFDC with cooperation and assistance needed to fulfill SFDC's obligation to assist SFDC's Customers in ensuring compliance with their obligation to carry out a data protection impact assessment or consult with regulators regarding Processing that is the subject of a data protection impact assessment, including by providing all relevant information, to the extent SFDC does not otherwise have access to the relevant information needed by SFDC's Customers and to the extent such information is available to Supplier.

2.7 **Records of Processing**. Upon SFDC's request, Supplier shall provide cooperation and assistance compiling or maintaining SFDC's records of processing as required by Data Protection Laws and Regulations. Supplier acknowledges that SFDC may be required, upon its supervisory authority's request, to make such records available to the supervisory authority.

2.8 **ISMS**. Supplier operates an information security management system (ISMS) for the Services in accordance with the ISO 27001 international standard.

3. TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

3.1 **Standard Contractual Clauses ("SCCs").** Supplier agrees that it shall abide by the relevant terms of the SCCs attached as Schedule 2 to this Vendor Privacy Exhibit. The SCCs shall apply to Supplier in its role as processor as if it were the "data importer." The SCCs shall apply to SFDC and, to the extent legally required, all of SFDC's Affiliates established within the European Economic Area, Switzerland and/or the United Kingdom, in their role as controllers and these entities shall be deemed "data exporters." In particular, Supplier agrees that as provided in the SCCs, individuals shall be third party beneficiaries to the SCCs. In addition, SFDC and Supplier hereby agree that the security provisions in the Agreement shall apply to Appendix 2 of the SCCs. To the extent SFDC is acting as Processor with respect to the Personal Data, then the parties agree that SFDC shall be entitled to exercise the rights under the SCCs on behalf of the Controller (as if it were the "data exporter") or to delegate such rights to the Controller and/or to procure from Supplier that Controller may directly exercise such rights with Supplier.

3.2 **EU-US and Swiss-US Privacy Shield Frameworks**. Supplier will:

a. Provide at least the same level of protection for Personal Data as is required by the relevant principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.
b. Promptly notify SFDC of any failure or inability to provide at least the same level of protection.
c. Where Supplier permits a Sub-processor to access Personal Data (subject to SFDC's approval right as set forth in the "Sub-processing" section), Supplier will require the Sub-processor to provide at least the same level of protection as is required by the relevant principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.

3.3 Binding Corporate Rules. If Supplier processes SFDC Customer Data, then Supplier acknowledges that SFDC has obtained approval of the Salesforce Processor Binding Corporate Rules ("BCR"), which is included as a legal transfer mechanism in the agreement with its Customers to cover any transfer of Personal Data outside of the European Union, the European Economic Area, their European Union's member states, or Switzerland. Supplier agrees that it shall abide by the relevant terms of the BCR, as updated from time to time, and as published at http://www.sfdcstatic.com/assets/pdf/misc/Salesforce-Processor-BCR.pdf, regarding such Personal Data.

4. SECURITY INCIDENT RESPONSE

4.1 Security Incident Response Program. Supplier maintains appropriate security incident management policies and procedures. Supplier will immediately, but at least within 24 hours upon discovery, notify SFDC of an actual or reasonably suspected Security Breach. In the notification, Supplier shall include details of when the Security Breach occurred and when it was detected, the nature and scope of the Protected Information involved in the Security Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the observed and probable consequences of the Security Breach, measures taken or proposed to mitigate the negative effects of the Security Breach, the name and contact details of the data protection officer or other contact point where more information can be obtained, and all other information requested by SFDC regarding the Security Breach. In addition, Supplier shall (i) investigate and remediate the effects of the Security Breach; (ii) provide SFDC, in writing, an impact assessment and assurance satisfactory to SFDC that such Security Breach will not recur; and (iii) upon SFDC's request, provide SFDC with cooperation and assistance needed to fulfill SFDC's obligations to provide information to regulators or individuals without undue delay as required by Data Protection Laws and Regulations. To the extent Supplier does not have full information about the Security Breach at the time of the initial notification, Supplier shall still complete the initial notification on the timing set forth above and then supplement that with additional information as it becomes available. Without limiting any other rights or remedies of SFDC, if as the result of any act or omission of Supplier or any of its personnel, contractors, or agents, one or more third parties is required to be notified of unauthorized access or use of Protected Information, Supplier agrees it shall be responsible for any reasonable costs associated with such communication (including providing call center services) and for any costs of providing a credit monitoring services. In addition, Supplier will provide indemnification to SFDC related to such Security Breach as set forth in the Agreement.

5. DATA STORAGE AND DELETION

5.1 Data Storage. Supplier will abide by the following with respect to storage of Protected Information and Confidential Information:

a. Supplier will not store or retain any Protected Information or Confidential Information except as necessary to perform Services under the Agreement.
b. Supplier will (i) inform SFDC in writing of all countries where Protected Information is Processed or stored and (ii) obtain consent from SFDC for Processing or storage in the identified countries. If Supplier processes SFDC Customer Data, SFDC may make this country list available to SFDC Customers.

5.2 Data Deletion. Supplier will abide by the following with respect to deletion of Protected Information and Confidential Information:

a. Within 30 calendar days of the Agreement's expiration or termination, or sooner if requested by SFDC, Supplier will securely destroy (per subsection (c) below) all copies of Protected Information and Confidential Information (including any automatically created archival copies).
b. Upon SFDC's request, Supplier will promptly return to SFDC a copy of all Protected Information and Confidential Information within 30 days and, if SFDC also requests deletion of the Protected Information and Confidential Information, will carry that out as set forth above.
c. All deletion of Protected Information and Confidential Information must be conducted in accordance with best practices for deletion of sensitive data. For example, secure deletion from a hard drive is defined at a minimum as a seven-pass write over the entire drive.
d. Tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method, such as shredding performed by a bonded provider.
e. Upon SFDC's request, Supplier will provide a "Certificate of Deletion" certifying that Supplier has deleted all Protected Information and Confidential Information. Supplier will provide the "Certificate of Deletion" within 30 days of SFDC's request.

6. SUB-PROCESSING

6.1 Consent for Sub-processing. Supplier will not sub-process any of its obligations under this Agreement except as set forth

in this Section. Supplier and SFDC shall agree to an initial list of approved Sub-processors. Supplier may add additional Sub-processors to this list provided that it gives 120 days' prior written notification of the identity of the Sub-processor to SFDC and SFDC does not object to the appointment within that period. In the event SFDC objects to a new Sub-processor, Supplier will use reasonable efforts to make available to SFDC a change in the affected Services or recommend a commercially reasonable change to SFDC's use of the affected Services to avoid Processing of Protected Information by the objected-to new Sub-processor without unreasonably burdening SFDC. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, SFDC may terminate the applicable Order Form(s) in respect to those Services which cannot be provided by Supplier without the use of the objected-to new Sub-processor, by providing written notice to Supplier, without Supplier imposing a penalty for such termination on SFDC. SFDC shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services. For the avoidance of doubt, sub-processing includes any Processing of Protected Information, including access, transmission, or storage by Supplier, its Affiliates, or its Sub-processors. Unless SFDC expresses in the consent an intent to allow Supplier to sub-process generally, any consent provided by SFDC per this section is limited to the specific Statement of Work and the specific Sub-processor for which the consent was provided. Supplier's use of Sub-processors shall be subject to the following:

a. Supplier shall be fully responsible for the performance of any Sub-processor and the compliance with all of the obligations of this Agreement by any Sub-processor. To this end, Supplier will conduct proper due diligence on all Sub-processors to ensure each Sub-processor can comply with Data Protection Laws and Regulations, all applicable terms and conditions of this Agreement, and all applicable SFDC policies and procedures to which Supplier may be subject during the term of this Agreement.
b. Sub-processors retained by Supplier to provide Services for SFDC will at all times be deemed Sub-processors of Supplier and shall not under any circumstance be construed or deemed to be employees or Sub-processors of SFDC.
c. Supplier shall ensure that it has a written contract in place with the relevant Sub-processor which meets the same obligations in respect of Processing of SFDC's Protected Information as are imposed on Supplier under this Vendor Privacy Exhibit.
d. Supplier shall flow down all obligations in this Agreement regarding, among other things: (i) Protected Information and (ii) all SFDC's and SFDC's regulator's (and, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's) rights regarding review and audit (including SFDC's right to appoint an independent third party to perform such review or audits).

6.2 **Copies of sub-processing agreements**. Upon SFDC's request, Supplier will provide SFDC copies of any sub-processing agreements it has in support of the provision of the Services. Supplier will provide such copies to SFDC within ten (10) days of SFDC's request. Supplier may remove any commercial information from such copies before providing such agreements to SFDC. SFDC may share such copies with SFDC Customers who request this information.

7. AUDITS

7.1 **Right to Audit; Permitted Audits.** In addition to any other audit rights described in the Agreement, SFDC and its regulators (and, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's) shall have the right to an on-site audit of Supplier's architecture, systems, policies and procedures relevant to the security and integrity of Protected Information, or as otherwise required by a governmental regulator:

a. Following any notice from Supplier to SFDC of an actual or reasonably suspected Security Breach or unauthorized disclosure of Protected Information.
b. Upon SFDC's reasonable belief that Supplier is not in compliance with its security policies and procedures under the Agreement regarding Protected Information.
c. As required by governmental regulators.
d. For any reason, or no reason at all, once annually.

7.2 **Audit Terms**. Any audits described in this Section shall be:

a. Conducted by SFDC or its regulator (or, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's), or through a third party independent contractor selected by one of these parties.
b. Conducted during reasonable times.
c. To the extent possible, conducted upon reasonable advance notice to Supplier.
d. Of reasonable duration and shall not unreasonably interfere with Supplier's day-to-day operations.

7.3 **Third Parties**. In the event that SFDC conducts an audit through a third party independent auditor or a third party accompanies SFDC or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Supplier's and Supplier's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

7.4 **Audit Results**. Upon Supplier request, after conducting an audit, SFDC shall notify Supplier of the manner in which Supplier does not comply with any of the applicable security, confidentiality or privacy obligations herein. Upon such notice, Supplier shall make any necessary changes to ensure compliance with such obligations at its own expense and without

unreasonable delay and shall notify SFDC when such changes are complete. Notwithstanding anything to the contrary in the Agreement, SFDC may conduct a follow-up audit within six (6) months of Supplier's notice of completion of any necessary changes. To the extent that a Supplier audit and/or SFDC audit identifies any material security vulnerabilities, Supplier shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. MISCELLANEOUS TERMS

8.1 **Legal Process**. If Supplier or anyone to whom Supplier provide access to Protected Information becomes legally compelled by a court or other government authority to disclose Protected Information, then to the extent permitted by law, Supplier will promptly provide SFDC with sufficient notice of all available details of the legal requirement and reasonably cooperate with SFDC's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as SFDC may deem appropriate.

8.2 **Conflict**. In the event of any conflict or inconsistency between this Vendor Privacy Exhibit and the Agreement, this Vendor Privacy Exhibit shall prevail.

8.3 **Disclosure of this Exhibit**. As required or upon request, SFDC may provide a summary or copy of this Vendor Privacy Exhibit to any government regulator or SFDC Customer.

8.4 **Survival**. Supplier's obligations under this Vendor Privacy Exhibit will survive expiration or termination of the Agreement and completion of the Services as long as Supplier continues to have access to Protected Information.

8.5 **Suspension**. SFDC may immediately suspend Supplier's Processing of Protected Information if Supplier is not complying with this Vendor Privacy Exhibit.

8.6 **Termination**. SFDC may terminate the Agreement or an applicable Order Form(s) if SFDC reasonably determines that (a) Supplier has failed to cure material noncompliance with the Vendor Privacy Exhibit within a reasonable time; or (b) SFDC needs to do so to comply with Data Protection Laws and Regulations.

List of Schedules

Schedule 1: Details of the Processing
Schedule 2: Standard Contractual Clauses

SCHEDULE 1 - DETAILS OF THE PROCESSING

Categories of Data Subjects

SFDC may provide Personal Data to Supplier 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 SFDC (who are natural persons)
- Employees or contact persons of SFDC's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of SFDC (who are natural persons)
- SFDC's users authorized by SFDC to use the Services

Categories and nature of Personal Data

SFDC may provide Personal Data to Supplier 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
- Localisation data

Scope and purpose of Processing

The objective of Processing of Personal Data by Supplier is the performance of the Services pursuant to the Agreement.

Duration of Processing

Subject to the Data Storage and Deletion section of the Vendor Privacy Exhibit, Supplier will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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: salesforce.com, inc.

Address: The Landmark @ One Market Street, 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 **exporter**)

And

[Contact information related to the data importer found in the Vendor Privacy Amendment]

(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;

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

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

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

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

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

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

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

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

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

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

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

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

Clause 6

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

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.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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 (as such term is applied *mutatis mutandis* per the Vendor Privacy Exhibit) is (please specify briefly your activities relevant to the transfer): Salesforce.com, inc. is a provider of enterprise cloud computing solutions.

Data importer

The data importer (as such term is applied *mutatis mutandis* per the Vendor Privacy Exhibit) is (please specify briefly activities relevant to the transfer):

Supplier provides the services as set forth in the Agreement.

Data subjects

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

Data exporter may submit personal data to the Service 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 Services 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
- Localisation 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 Services, 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 Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses:

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 will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data contained in Customer Data, as described in the Vendor Privacy Exhibit. Data Importer will not materially decrease the overall security of the Services during the term of the Agreement.