DATA PROCESSING ADDENDUM
(EU Standard Contractual Clauses)

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement between Customer and FFDC (the "Agreement") to reflect the parties' agreement with regard to the Processing of Customer Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of three parts: the main body of the DPA, Attachment 1 (including Appendices 1 to 3), and Attachment 2.
2. This DPA has been pre-signed on behalf of FFDC. The Standard Contractual Clauses in Attachment 1 have been presigned by FinancialForce.com, inc.
3. To complete this DPA, Customer must: (a) complete the information in the signature box and sign on page 5, (b) complete the information regarding the data exporter on page 6, and (c) complete the information in the signature box and sign on pages 11 and 13.
4. Submit the completed and signed DPA to FFDC via privacy@financialforce.com.

Upon receipt of the validly completed DPA at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the FinancialForce.com entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with FFDC or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the FinancialForce.com entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement execute this DPA, and Affiliates of such Customer entity will benefit under this DPA via Clause 9.1(b) below.

This DPA shall not replace any additional rights relating to Processing of Customer Data previously negotiated by Customer in the Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

In the course of providing the Services to Customer pursuant to the Agreement, FFDC may Process Personal Data on behalf of Customer. FFDC agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services or collected and Processed by or for Customer using the Services.

1. DEFINITIONS

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

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

"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, applicable to the Processing of Personal Data under the Agreement.

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

"FFDC" means the FinancialForce.com entity or branch which is a party to this DPA, as specified in the clause "HOW THIS DPA APPLIES" above, being FinancialForce.com, inc., a company incorporated in Delaware, U.S.A., FinancialForce.com UK Branch, a UK branch of FinancialForce.com, inc., FinancialForce.com Canada, Inc., a company incorporated in Ontario,

Canada (successor-in-interest to Vana Group Inc.), or FinancialForce.com (SCM), inc., a company incorporated in Delaware (successor-in-interest to Less Software Incorporated), as applicable.

"FFDC Group" means FFDC and its Affiliates engaged in the Processing of Personal Data.

"Personal Data" means any information relating to an identified or identifiable person where such data is submitted to the Services as Customer Data.

"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, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Standard Contractual Clauses" means the agreement executed by and between Customer and FinancialForce.com.com, inc. and attached hereto as Attachment 1 pursuant to the European Commission's decision 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 Data Processor engaged by FFDC, by a member of the FFDC Group or by another Sub-processor.

"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.

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 Data Controller, FFDC is a Data Processor and that FFDC or members of the FFDC Group will engage Sub-processors pursuant to clause 5 "Sub-processors" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the 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 **FFDC's Processing of Personal Data.** FFDC shall only Process Personal Data on behalf of and in accordance with Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs FFDC to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3. RIGHTS OF DATA SUBJECTS

3.1 **Correction, Blocking and Deletion.** To the extent Customer, in its use of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, FFDC shall comply, or cause the applicable Sub-processor to comply, with any commercially reasonable request by Customer to facilitate such actions to the extent FFDC, or the Sub-processor as applicable, is legally permitted to do so. To the extent legally permitted, Customer shall be responsible for any costs arising from FFDC's provision of such assistance.

3.2 **Data Subject Requests.** FFDC shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to or correction, amendment or deletion of that person's Personal Data. FFDC shall not respond to any such Data Subject request without Customer's prior written consent save to confirm that the request relates to Customer or as otherwise required by law. FFDC shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use of the Services. If legally permitted, Customer shall be responsible for reasonable costs, if any, incurred by FFDC to provide such assistance.

4. FFDC PERSONNEL

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

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

4.3 **Limitation of Access.** FFDC shall ensure that FFDC's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4 **Data Protection Officer.** Members of the FFDC Group have appointed a data protection officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at privacy@financialforce.com.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) FFDC's Affiliates may be retained as Sub-processors; and (b) FFDC and FFDC's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

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

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** FFDC shall maintain administrative, physical and technical safeguards designed to protect the security, confidentiality and integrity of Customer Data, including Personal Data, in accordance with Appendix 2 to Attachment 1. FFDC will not materially decrease the overall security of the Services during the term of the Agreement.

6.2 **SOC 1 Report.** Upon Customer's written request no more frequently than once annually, FFDC shall provide to Customer a copy of FFDC's then most recent service organization controls (SOC) 1 report for the Services. FFDC may require Customer to sign a nondisclosure agreement reasonably acceptable to FFDC before FFDC provides a copy of such report to Customer.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

FFDC maintains a security incident management procedure and shall, to the extent permitted by law, promptly notify Customer of any actual or reasonably suspected unauthorised disclosure of Customer Data, including Personal Data, by FFDC or its Sub-processors of which FFDC becomes aware (a "Security Breach"). To the extent such Security Breach is caused by a violation of the requirements of this DPA by FFDC, FFDC shall make reasonable endeavours to identify and remediate the cause of such Security Breach.

8. RETURN AND DELETION OF CUSTOMER DATA

FFDC shall return Customer Data to Customer and delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

9. ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses in Attachment 1 (the "Standard Contractual Clauses") and the additional terms in this Clause 9 will apply to the Processing of Personal Data by FFDC in the course of providing the Services listed in Appendix 3 to the Standard Contractual Clauses (the "SCC Services").

(a) The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive), and (ii) not covered by a suitable framework recognised by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors.

(b) The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter, and (ii) all Affiliates of Customer established within the EEA and Switzerland that have purchased SCC Services on the basis of an Order Form or are using SCC Services in accordance with the Agreement. For the purpose of the Standard Contractual Clauses and this Clause 9, the aforementioned entities shall be deemed "Data Exporters".

9.2 **Objective and Duration.** The objective of Processing of Personal Data by FFDC is the performance of the SCC Services pursuant to the Agreement.

9.3 **Instructions.** This DPA and the Agreement are Customer's complete and final instructions to FFDC 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 Customer to process Personal Data: (a) processing in accordance with the Agreement and applicable Order Form(s); and (b) processing initiated by Users in their use of the SCC Services.

9.4 **Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that FFDC's Affiliates may be retained as Sub-processors; and (b) FFDC and FFDC's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services.

(a) **List of Current Sub-processors and Notification of New Sub-processors.** A list of Sub-processors for the SCC Services as of the Effective Date is attached as Attachment 2. Upon request, FFDC shall make available to Customer an updated list of Sub-processors for the SCC Services with the identities of those Sub-processors ("Updated Sub-processor List").

(b) **Objection Right for new Sub-processors.** If Customer has a reasonable basis to object to FFDC's use of a new Sub-processor identified on an Updated Sub-processor List, Customer shall so notify FFDC promptly in writing within 10 business days after Customer first receives such Updated Sub-processor List identifying the new Sub-processor. In the event Customer objects to a new Sub-processor(s) and that objection is not unreasonable FFDC will use reasonable endeavours to make available to Customer a change in the affected SCC Services or recommend a commercially reasonable change to Customer's configuration or use of the affected SCC Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If FFDC is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) in respect only of those SCC Services which cannot be provided by FFDC without the use of the objected-to new Sub-processor, by providing written notice to FFDC. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated SCC Services.

(c) The parties agree that the copies of the Sub-processor agreements that must be sent by FFDC 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 FFDC beforehand; and, that such copies will be provided by FFDC only upon reasonable request by Customer.

9.5 **Audits and Certifications.** The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, FFDC shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of FFDC and that has signed nondisclosure agreement reasonably acceptable to FFDC) information regarding the FFDC Group's compliance with the obligations set forth in this DPA in the form of FFDC's SOC1 report and, for its Sub-processors Salesforce.com, inc. and its subsidiaries, the third-party certifications and audits set forth in the Salesforce.com Security, Privacy and Architecture Documentation for the Salesforce Services available through the "Trust and Compliance" page on help.salesforce.com, to the extent Salesforce.com makes them generally available to its customers. Following any notice by FFDC to Customer of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Customer's reasonable belief that FFDC is in breach of its obligations in respect of protection of Personal Data under this DPA, or if such audit is required by Customer's Supervisory Authority, Customer may contact FFDC in accordance with the "Notices" Clause of the Agreement to request an audit at FFDC's premises of the procedures relevant to the protection of Personal Data. Any such request shall occur no more than once annually, save in the event of an actual or reasonably suspected unauthorised access to Personal Data. Customer shall reimburse FFDC for any time expended for any such on-site audit at the FFDC Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and FFDC shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by FFDC. Customer shall promptly notify FFDC with information regarding any non-compliance discovered during the course of an audit.

9.6 **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by FFDC to Customer only upon Customer's request.

9.7 **Conflict.** In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail.

10. PARTIES TO THIS DPA

The Clause "HOW THIS DPA APPLIES" specifies which FinancialForce.com entity is party to this DPA (FFDC). In addition, FinancialForce.com, inc. is a party to the Standard Contractual Clauses in Attachment 1. Notwithstanding the signatures below of any other FinancialForce.com entity, such other FinancialForce.com entities are not a party to this DPA or the Standard Contractual Clauses. If FinancialForce.com, inc. is not a party to the Agreement, the clause of the Agreement 'Limitation of Liability' shall apply as between Customer and FinancialForce.com, inc., and in such respect any reference to 'FFDC' shall include both FinancialForce.com, inc. and the FinancialForce.com entity that is a party to the Agreement.

11. LEGAL EFFECT

This DPA shall only become legally binding between Customer and FFDC (and FinancialForce.com, inc., if different) when the formalities steps set out in the Clause "HOW TO EXECUTE THIS DPA" above have been fully completed.

CUSTOMER

Customer Legal Name: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

FINANCIALFORCE.COM, INC.

Signature: DocuSigned by: 3B4FB80599D74B7...

Printed Name: Jeremy Roche

Title: President and Chief Executive Officer

Date: October 21, 2015 | 8:12 AM GMT

FINANCIALFORCE.COM UK BRANCH, a UK Branch of FINANCIALFORCE.COM, INC.

Signature: DocuSigned by: 3B4FB80599D74B7...

Printed Name: Jeremy Roche

Title: President and Chief Executive Officer

Date: October 21, 2015 | 8:12 AM GMT

FINANCIALFORCE.COM CANADA, INC.

Signature: DocuSigned by: 3B4FB80599D74B7...

Printed Name: Jeremy Roche

Title: Chief Executive Officer

Date: October 21, 2015 | 8:12 AM GMT

FINANCIALFORCE.COM (SCM), INC.

Signature: DocuSigned by: 3B4FB80599D74B7...

Printed Name: Jeremy Roche

Title: President

Date: October 21, 2015 | 8:12 AM GMT

ATTACHMENT 1

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: FinancialForce.com, inc.

Address: 595 Market Street, Suite 2700, San Francisco, CA 94105, USA

Tel.: + 1-866-743-2220; fax: ; e-mail: privacy@financialforce.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;

(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; and

(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 fulfill 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): Jeremy Roche

Position: President and Chief Executive Offier

Address: 595 Market Street, Suite 2700, San Francisco, CA 94105, USA

Other information necessary in order for the contract to be binding (if any):

Signature…… DocuSigned by: 3B4FB80599D74B7……
(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the 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):

The data exporter is (i) the legal entity that has executed the attached Standard Contractual Clauses as a data exporter, and (ii) all Affiliates of Customer established within the European Economic Area (EEA) and Switzerland that have purchased SCC Services on the basis of one or more Order Forms or are using SCC Services in accordance with the Agreement. The terms "Affiliate," "Customer" and "Order Form" are defined in the Agreement, and the terms "Agreement" and "SCC Services" are defined in the attached DPA.

Data importer

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

FinancialForce.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 Agreement.

Data subjects

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

Data exporter may submit Personal Data to the SCC 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 exporters' prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorised 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 SCC 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
- 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 SCC 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 SCC Services pursuant to the Agreement.

DATA EXPORTER

Name: …… 

Authorised Signature …… 

DATA IMPORTER

Name: Jeremy Roche

Authorised Signature …… 

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the 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):

1. **General Controls.** FFDC will implement, or be responsible for its Sub-processor's implementation of, measures designed to:
   - **(a)** deny unauthorised persons access to data-processing equipment used for processing Personal Data (equipment access control);
   - **(b)** prevent the unauthorised reading, copying, modification or removal of data media containing Personal Data (data media control);
   - **(c)** prevent unauthorised inspection, modification or deletion of stored Personal Data (storage control);
   - **(d)** prevent the use of automated data-processing systems by unauthorised persons using data communication equipment used to process Personal Data (user control);
   - **(e)** limit access to Personal Data by persons authorised to use an automated data-processing system to the scope and duration of their access authorisation (data access control);
   - **(f)** enable verification of the individuals to whom Personal Data has been transmitted or made available using data communication equipment (communication control);
   - **(g)** enable verification of which individuals input Personal Data into automated data-processing systems and when (input control);
   - **(h)** prevent the unauthorised reading, copying, modification or deletion of Personal Data during transfers of that data or during transportation of data media (transport control);
   - **(i)** enable restoration of installed systems used to process Personal Data in case of interruption (recovery);
   - **(j)** ensure that the functions of the system used to process Personal Data perform, that the appearance of faults in the functions is reported (reliability) and prevent stored Personal Data from corruption by means of a malfunctioning of the system (integrity).
2. **Personnel.** FFDC will take reasonable steps to ensure that no person shall be appointed by FFDC to process Personal Data unless that person:
   - **(a)** is competent and qualified to perform the specific tasks assigned to him by FFDC;
   - **(b)** has been authorised by FFDC; and
   - **(c)** has been instructed by FFDC in the requirements relevant to the performance of the obligations of FFDC under these Clauses, in particular the limited purpose of the data processing.
3. **Copy Control.** FFDC shall not make copies of Personal Data save as reasonably necessary to provide the Services and for backup purposes.
4. **Security Controls.** The Services include a variety of configurable security controls that allow Customer to tailor the security of the Services for its own use. These controls include:
   - Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
   - Controls to revoke access after several consecutive failed login attempts.
   - The ability to specify the lockout time period.
   - Controls on the number of invalid login requests before locking out a User.
   - Controls to ensure generated initial passwords must be reset on first use.
   - Controls to force a User password to expire after a period of use.
   - Controls to terminate a User session after a period of inactivity.
   - Password history controls to limit password reuse.
   - Password length controls.
   - Password complexity requirements (requires letters and numbers).
   - Verification question before resetting password.

- The ability to accept logins to the Services from only certain IP address ranges.
- The ability to restrict logins to the Services to specific time periods (Developer Edition, Enterprise Edition, and Unlimited Edition only).
- Ability to delegate user authentication or federate authentication via SAML.

5. **Security Procedures, Policies and Logging.** The Services are operated in accordance with the following procedures to enhance security:

   - User access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
   - If there is suspicion of inappropriate access, FFDC or its Sub-processor can provide Customer log entry records to assist in forensic analysis. This service will be provided to Customer on a time and materials basis.
   - Logging will be kept for a minimum of 90 days.
   - Logging will be kept in a secure area to prevent tampering.
   - Passwords are not logged under any circumstances.
   - Certain administrative changes to the Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Log" and are available for viewing by Customer's system administrator. Customer may download and store this data locally.
   - FFDC personnel will not set a defined password for a User. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting User.

6. **Intrusion Detection.** FFDC, or an authorised third party (subject to the terms of these Clauses), will monitor the Services for unauthorised intrusions using network-based intrusion detection mechanisms.

7. **User Authentication.** Access to the Services requires a valid User ID and password combination. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

8. **Security Logs.** FFDC shall ensure that all FFDC or Sub-processor systems used to store Customer Data, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralised syslog server (for network systems).

9. **Incident Management.** FFDC maintains security incident management policies and procedures. FFDC will promptly notify Customer in the event FFDC becomes aware of an actual or reasonably suspected unauthorised disclosure of Personal Data.

10. **Physical Security.** FFDC's Sub-processor's production data centres have an access system that controls access to the data centre. This system permits only authorised personnel to have access to secure areas. The facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, biometric access screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

11. **Reliability and Backup.** All networking components, load balancers, Web servers and application servers that are part of the SFDC Force.com platform are configured in a redundant configuration. All Personal Data is stored on a primary database server that is clustered with a backup database server for redundancy. All Personal Data is stored on carrier-class disk storage using RAID disks and multiple data paths. All Personal Data, up to the last committed transaction, is automatically backed up on a regular basis. Any backup tapes are verified for integrity stored in an offsite facility in a secure, fire-resistant location.

12. **Disaster Recovery.** FFDC will ensure that the systems where Customer Data is stored have a disaster recovery facility that is geographically remote from its primary data centre, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centre were to be rendered unavailable. FFDC will ensure that its Sub-processor that stores Customer Data has disaster recovery plans in place and tests them at least once per year.

13. **Viruses.** The Services will not introduce any viruses to Customer's systems; however, the Services do not scan for viruses that could be included in attachments or other Personal Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Service.

14. **Data Encryption.** The Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, Customer Data is encrypted during transmission between data centres for replication purposes.

15. **System Changes and Enhancements.** FFDC plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. FFDC will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

- FinancialForce Accounting
- FinancialForce Billing
- FinancialForce Fixed Assets
- FinancialForce Human Capital Management
- FinancialForce Media
- FinancialForce Professional Services Automation
- FinancialForce Revenue Recognition
- FinancialForce Service Contracts
- FinancialForce Supply Chain Management

Attachment 2

Sub-processors as of Effective Date of this DPA

Entity Name	Entity Type	Entity Country
FinancialForce.com Australia Pty Ltd	FFDC Affiliate [1]	Australia
FinancialForce.com Spain NL	FFDC Affiliate [1]	Spain
Salesforce.com, inc.	Third-Party Service Provider: Service Hosting [2]	United States
SFDC EMEA Data Centre Limited	Third-Party Service Provider: Service Hosting [2]	UK
SFDC Germany Data Centre GmbH	Third-Party Service Provider: Service Hosting [2]	Germany
SFDC France Data Centre Sarl	Third-Party Service Provider: Service Hosting [2, 3]	France
Kabushiki Kaisha salesforce.com (salesforce.com Co., Ltd.)	Third-Party Service Provider: Service Hosting [2]	Japan
Metacube Software, Pvt. Ltd.	Third-Party Service Provider: Customer Support [1]	India

1 These entities assist in the provision of customer support, and only have access to Customer Data to the extent Customer's Users expressly grant such access via the Services.

2 Salesforce.com, inc. and its subsidiaries host the Services and store all Customer Data. For customers based in the Americas, Europe, Middle East, and Africa, Salesforce.com stores customer data in its U.S. and/or European data centres. For customers based in the Asia Pacific region and Japan, Salesforce.com stores customer data in its Japan and U.S. data centres. To determine which data centres are used for a given customer, please see the Security, Privacy and Architecture Documentation for the Salesforce Services by visiting the "Trust and Compliance" page on help.salesforce.com. Salesforce.com may update the foregoing policies from time to time, provided that Salesforce.com will not relocate storage of Customer's Customer Data to a country where it is not already storing the Customer Data, without Customer's prior written consent. Salesforce.com may store in all data centres identifying information about Customer's instance(s) of the Services and identifying information about Users for the purposes of operating the Services, such as facilitating the login process. Such identifying information shall only include the following personal data about Users, as provided by Customer in its provision of User accounts: first and last name, email address, username, phone number, and physical business address.

3 Salesforce.com plans to open the data centre in France in 2016.