DATA PROCESSING ADDENDUM
(GDPR and EU Standard Contractual Clauses)

(Rev. 25 January 2018)

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement or other written or electronic agreement between FinancialForce ("**FF**") and Customer for the purchase of online services (including associated FF offline or mobile components) from FF (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

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

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

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3, and 4 (including Appendices 1 to 3).
2. This DPA has been pre-signed on behalf of FF. The Standard Contractual Clauses in Schedule 5 have been presigned by salesforce.com, inc. as the data importer.
3. To complete this DPA, Customer must:
   a. Complete the information as the data exporter on pages 12 and 18.
   b. Complete the information in the signature box and sign on pages 7, 17 and 19.
4. Send the completed and signed DPA to FF at privacy@financialforce.com. Upon receipt of the validly completed DPA by FF 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 FF 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 FF 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 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.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

1. DEFINITIONS

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

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and FF, but has not signed its own Order Form with FF and is not a "Customer" as defined under the Agreement.

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

"Customer Data" means what is defined in the Agreement as "Customer Data." or "Your Data."

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement.

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

"FF" means the FinancialForce entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being FinancialForce.com, Inc., a company incorporated in Delaware, U.S.A, FinancialForce.com Canada, Inc., a company incorporated in Ontario, Canada, or FinancialForce UK Limited, a company registered in England and Wales, as applicable.

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

"GDPR" means the 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 (General Data Protection Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"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.

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

"Standard Contractual Clauses" means the agreement executed by and between Customer and FinancialForce UK Limited 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 Processor engaged by FF, by a member of the FF Group or by another Sub-processor.

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

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, FF is a Processor and that FF or members of the FF 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 FF's Processing of Personal Data. FF shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's instructions 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.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by FF is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 3 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** FF shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to access, correct or delete that person's Personal Data or if a Data Subject objects to the Processing thereof ("Data Subject Request"). FF shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Customer to which Customer hereby agrees. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, FF shall upon Customer's request provide commercially reasonable assistance to facilitate such Data Subject Request to the extent FF is legally permitted to do so and provided that such Data Subject Request is exercised in accordance with Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from FF's provision of such assistance.

3.2 **Data Subject Request.** With effect from 25 May 2018, the following wording will replace Clause 3.1 ("Data Subject Request") in its entirety: *Data Subject Requests. FF shall, to the extent legally permitted, promptly notify Customer if FF receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, FF shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, FF shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent FF is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from FF's provision of such assistance.*

4. FF PERSONNEL

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

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

4.3 **Limitation of Access.** FF shall ensure that FF'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 FF Group will appoint 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) FF's Affiliates may be retained as Sub-processors; and (b) FF and FF's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. FF or a FF Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.** A list of Sub-processors as of 25 January 2018 for the Services listed in Appendix 3 to the Standard Contractual Clauses is attached in Schedule 1 (Sub-processors as of 25 January 2018). Upon request, FF shall make available to Customer an updated list of Sub-processors for the SCC Services with the identities of those Sub-processors and their country of location ("**Updated Sub-processor List**").

5.3 **Objection Right for New Sub-processors.** Customer may object to FF's use of a new Sub-processor by notifying FF in writing within ten (10) business days after receipt of an Updated Sub-processor List. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, FF will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If FF is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by FF without the use of the objected-to new Sub-processor, by providing written notice to FF. FF will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following

the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 **Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be sent by FF 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 the FF beforehand; and, that such copies will be provided by FF only upon reasonable request by Customer.

5.5 **Liability**. FF shall be liable for the acts and omissions of its Sub-processors to the same extent FF 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.** FF shall maintain administrative, physical and technical safeguards designed for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, including Personal Data, in accordance with Appendix 2 to Schedule 4 (Standard Contractual Clauses). FF will not materially decrease the overall security of the Services during a subscription term.

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

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

FF maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by FF or its Sub-processors of which FF becomes aware (a "**Customer Data Incident**"). FF shall make reasonable endeavours to identify the cause of such Customer Data Incident and take those steps as FF deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within FF's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. RETURN AND DELETION OF CUSTOMER DATA

FF shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between FF and each such Authorized Affiliate subject to the provisions of the Agreement, this Clause 9, and Clause 10 below. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement, and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with FF under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

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

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against FF directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate

individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Clause 9.3.2, below).

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

10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and FF, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" clause of the Agreement, and any reference in such clause to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, FF's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and any Appendices thereto.

11. EUROPE-SPECIFIC PROVISIONS

11.1 GDPR. With effect from 25 May 2018, FF will Process Personal Data in accordance with the GDPR requirements directly applicable to FF's provision of its Services.

11.2 Data Protection Impact Assessment. With effect from 25 May 2018, upon Customer's request, FF shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to FF. FF shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Clause 9.2, to the extent required under the GDPR.

11.3 Transfer Mechanisms for Data Transfers. Subject to the terms of this DPA (including Clauses 11.4 and 11.5 below), FF makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out below in this Clause 11.3, to any online transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. FF'S EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications apply to the Services listed in Schedule 2 (EU-US and Swiss-US Privacy Shield Services) to this DPA (the "**EU-US and Swiss-US Privacy Shield Service**s"), subject to the additional terms in Clause 11.4 below;
2. The Standard Contractual Clauses set forth in Schedule 4 to this DPA apply to the Services listed in Appendix 3 to the Standard Contractual Clauses (the "**SCC Services**"), subject to the additional terms in Clause 11.5 below.

In the event that Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) FF's EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications and, (2) the Standard Contractual Clauses.

11.4 Additional Terms for EU-US and Swiss-US Privacy Shield Services. FinancialForce.com, Inc. self-certifies to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce, and FinancialForce.com, Inc. shall ensure that it maintains its self-certification to and compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to the Processing of Personal Data that is transferred from the European Economic Area and/or Switzerland to the United States.

11.5 Additional Terms for SCC Services.

11.5.1 Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Claus 11.5 1 apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the SCC Services. For the purpose of the Standard Contractual Clauses and this Clause 11.5, the aforementioned entities shall be deemed "data exporters".

11.5.2 **Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to FF for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the SCC Services and (c) 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.

11.5.6 **Appointment of New Sub-processors and List of Current Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) FF's Affiliates may be retained as Sub-processors; and (b) FF and FF's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. FF shall make available to Customer the current list of Sub-processors in accordance with Clause 5.2 of this DPA

11.5.7 **Notification of New Sub-processors and Objection Right for New Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that FF may engage new Sub-processors as described in Clauses 5.2 and 5.3 of the DPA.

11.5.8 **Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by FF 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 FF beforehand; and, that such copies will be provided by FF, in a manner to be determined in its discretion, only upon request by Customer.

11.5.9 **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, FF shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of FF and that has signed nondisclosure agreement reasonably acceptable to FF) information regarding the FF Group's compliance with the obligations set forth in this DPA in the form of FF's SOC 1 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 located at https://help.salesforce.com/articleView?id=Trust-and-Compliance-Documentation&language=en_US&type=1 to the extent salesforce.com makes them generally available to its customers. Following any notice by FF to Customer of an actual or reasonably suspected unauthorized disclosure of Personal Data, upon Customer's reasonable belief that FF 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 FF in accordance with the "Notices" Clause of the Agreement to request an audit at FF'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 FF for any time expended for any such on-site audit at the FF 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 FF 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 FF. Customer shall promptly notify FF with information regarding any non-compliance discovered during the course of an audit.

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

11.5.11 **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 4, the Standard Contractual Clauses shall prevail.

12. PARTIES TO THIS DPA

The Section "HOW THIS DPA APPLIES" specifies which FF entity is party to this DPA. In addition, FinancialForce.com, Inc. is a party to the Standard Contractual Clauses in Schedule 4. Notwithstanding the signatures below of any other FF entity, such other FF entities are not a party to this DPA or the Standard Contractual Clauses. Where FF is a different legal entity than FinancialForce.com, Inc., FF is carrying out the obligations of the data importer as set out in Schedule 4 "Standard Contractual Clauses" on behalf of FinancialForce.com, Inc.

13. LEGAL EFFECT

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

List of Schedules

Schedule 1: Sub-processors as of 30 July 2017

Schedule 2: EU-US and Swiss-US Privacy Shield Services

Schedule 3: Details of the Processing

Schedule 4: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER

Signed: _____

Name: _____

Title: _____

Date: _____

FINANCIALFORCE.COM, INC.

Signed: DocuSigned by: 23AA52D2EAAC48A...

Name: John J. Moss

Title: SVP and General Counsel

Date: January 25, 2018

FINANCIALFORCE UK LIMITED

Signed: DocuSigned by: 23AA52D2EAAC48A...

Name: John J. Moss

Title: Director

Date: January 25, 2018

FINANCIALFORCE.COM CANADA, INC.

Signed: DocuSigned by: Tod Nielsen E1ECC29F1E1248C...

Name: Tod Nielsen

Title: Chief Executive Officer

Date: January 25, 2018

SCHEDULE 1

Sub-processors as of 25 January 2018

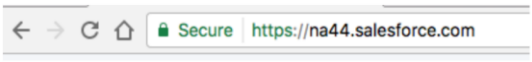
(Please check the "Infrastructure – Customer Data Storage" Section of the Salesforce Sub-processors List at https://help.salesforce.com/articleView?id=Salesforce-Services-Trust-and-Compliance-Documentation&language=en_US&type=1 for updated information)

Infrastructure – Customer Data Storage

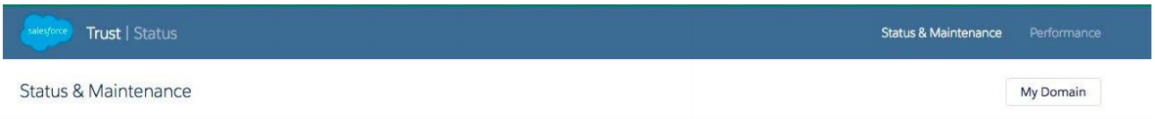
The Services are hosted in enterprise-class data centres and are divided into a modular architecture based on "instances." Except in the scenarios described below, access to the infrastructure used to store data submitted by customers to the Services ("Customer Data") is owned or controlled by Salesforce. In general, Customer Data is stored in data centres in the region from which a customer subscribes to the Services; however, customers can request at the time of sign-up to be hosted in a different region. For customers based in the Americas, Salesforce stores Customer Data in its data centres located in the United States. For customers based in Europe, the Middle East, and Africa (EMEA), Salesforce stores Customer Data in its data centres located in Europe. For customers based in the Asia Pacific (APAC) region, including Japan and Australia, Salesforce stores Customer Data in its data centres in Japan and, for some customers, the U.S. Additionally, certain customers in Canada and Australia may have the option to subscribe to Services hosted on the infrastructure of a third-party hosting provider ("Public Cloud Infrastructure"); for customers using Public Cloud Infrastructure, Salesforce stores Customer Data in data centres operated by Amazon Web Services, Inc. ("AWS").

Each instance (for example, NA10 or CS2) of the Services contains many servers and other elements to make it run. Copies of each instance are located in two data centres. One data center serves as the primary location from which data is served, and the second data center serves as a back-up. The primary location will switch between the two data centres periodically. Salesforce uses vendor-supplied technologies to optimize the accuracy and integrity of replication between primary and secondary systems and to continuously monitor the data replication process.

The instance your organization uses is indicated in the browser's address bar, shown highlighted below.



Alternatively, if your organization uses the Force.com Platform's My Domain feature, you can determine what instance your organization is on by accessing the My Domain lookup feature available at https://status.salesforce.com. At the top of the page there is a My Domain button; clicking on the My Domain button will open up a search box where you can input you're my Domain, click search, then navigate to the detail page for your Salesforce instance.



The following describes the countries and legal entities engaged in the storage of Customer Data by FF for the Services.

Customer Region	Instance Type	Data Centre Countries and Operators
Americas	All NA instances other than NA 99	United States (salesforce.com, inc.)
	All Sandboxes not listed below	
	NA99	Canada (Amazon Web Services, Inc.) * * For customers based in Canada using Public Cloud Infrastructure.
	Sandbox CS98, CS99	
APAC	AP0, AP1, AP2	Japan (Kabushiki Kaisha salesforce.com, also known as

	Sandbox CS5, CS6, CS31	salesforce.com Co., Ltd.)
	AP3, AP4, AP5	Japan (Kabushiki Kaisha salesforce.com, also known as salesforce.com Co., Ltd.) United States (salesforce.com, inc.)
	Sandbox CS57, CS58	
	AP9	Australia (Amazon Web Services, Inc.) * * For customers based in Australia using Public Cloud Infrastructure
	Sandbox CS115, CS116	
EMEA	EU0, EU1, EU4, EU6	United Kingdom (SFDC EMEA Data Centre Limited) Germany (SFDC Germany Data Center GmbH)
	Sandbox CS81, CS82, CS83, CS86, CS87	
	Sandbox CS80	France (SFDC France Data Centre Sarl) United Kingdom (SFDC EMEA Data Centre Limited)
	EU7, EU8, EU9, EU10, EU11, EU12, EU13, EU14, EU15	Germany (SFDC Germany Data Centre GmbH) France (SFDC France Data Centre Sarl)
	Sandbox CS84, CS85, CS88, CS89	

FF 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 and the provision of customer support. 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.

Sandbox copies are created at a data centre level; any instance can refresh to any sandbox within a data centre. Sandbox copies in a Salesforce-operated data centre may be redirected to another Salesforce-operated data centre in the same region if necessary, to maintain performance levels. As an example, an EMEA-based sandbox instance could redirect to another EMEA data centre.

Each instance of Einstein Analytics is run as a shared services (instance group) environment consisting of servers and other elements supporting multiple instances. Einstein Analytics is accessible only through anauthenticated connection from an instance of the Services. Instance groups reside geographically in the same data centres as your organization's primary Services / Force.com Platform instance (e.g., AP0, NA2). Customer Data submitted to Einstein Analytics is backed up in your organization's unique instance of the Services / Force.com Platform; geographically, in the data centres as per the table above.

Customer Support

The following legal entities are engaged in processing Customer Data for customer support purposes. The entities below only have access to Customer Data to the extent such access is expressly granted by Customer for support purposes. Such entities may also have access to the following identifying information about Users for the purpose of routing and facilitating customer support requests: first and last name, email address, username, phone number, and physical business address.

Entity Name	Entity Type	Entity Country
FinancialForce.com, Inc.	FF Affiliate	United States
FinancialForce.com Australia Pty Ltd	FF Affiliate	Australia

FinancialForce.com Canada, Inc.	FF Affiliate	Canada
FinancialForce Spain SL	FF Affiliate	Spain
FinancialForce UK Limited	FF Affiliate	United Kingdom
Metacube Software, Pvt. Ltd.	Third-Party Service Provider: Customer Support	India

SCHEDULE 2

EU-US and Swiss-US Privacy Shield Services

- Financials (Accounting)
- Supply Chain Management
- Service Contracts
- Revenue Recognition
- Billing
- Professional Services Automation (PSA)
- Human Capital Management
- Financial Management Community
- PSA Community

SCHEDULE 3

Details of the Processing

Nature and Purpose of Processing

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

Duration of Processing

Subject to Clause 8 of the DPA, FF will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

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

- Customers, business partners, vendors and subcontractors of Customer (who are natural persons)
- Employees or contact persons of Customer's customers, business partners, vendors and subcontractors
- Employees, agents, advisors, contractors, and freelancers of Customer (who are natural persons), and their family members
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

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

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Professional skills information
- Personal life data
- Health and medical information
- Compensation information
- Connection data
- Localisation data

SCHEDULE 4

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

[CUSTOMER: PLEASE COMPLETE]

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, California 94105

Tel.: + 1-866-743-2220 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 fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have

factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

[CUSTOMER: PLEASE COMPLETE AND SIGN:]

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): John J. Moss

Position: SVP and General Counsel

Address: 595 Market Street, Suite 2700, San Francisco, California 94105

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

DocuSigned by:
23AA52D2EAAC48A...

Signature…….
(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

[CUSTOMER: PLEASE COMPLETE:]

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

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 data exporter may submit Personal Data to the 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, vendors and subcontractors of the data exporter (who are natural persons)
- Employees or contact persons of the data exporter's customers, business partners, vendors and subcontractors
- Employees, agents, advisors, freelancers of the data exporter (who are natural persons), and their family members
- The data exporter's Users authorized by the data exporter to use the Services

Categories of Data

The data exporter may submit Personal Data to the 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
- Professional skills information
- Personal life data
- Health and medical information
- Employee compensation information
- Connection data
- Localisation data

Special categories of data (if appropriate)

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

The 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, trade-union membership, and the processing of data concerning health.

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.

[CUSTOMER: PLEASE SIGN]

DATA EXPORTER

Name: …….

Authorised Signature ……..

DATA IMPORTER

Name: John J. Moss

Authorised Signature …… DocuSigned by: 23AA52D2EAAC48A...

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.** FF shall 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 the unauthorised input of Personal Data and the 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)** ensure that persons authorised to use an automated data-processing system only have access to the Personal Data covered by their access authorisation (data access control);
   - **(f)** ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
   - **(g)** ensure that it is subsequently possible to verify and establish which Personal Data have been put into automated data-processing systems and when and by whom the input was made (input control);
   - **(h)** prevent the unauthorised reading, copying, modification or deletion of Personal Data during transfers of those data or during transportation of data media (transport control);
   - **(i)** ensure that installed systems used to process Personal Data may, in case of interruption, be restored (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 to prevent stored Personal Data from corruption by means of a malfunctioning of the system (integrity).
2. **Personnel.** FF shall take reasonable steps to ensure that no person shall be appointed by FF to process Personal Data unless that person:
   - **(a)** is competent and qualified to perform the specific tasks assigned to him by FF;
   - **(b)** has been authorised by FF; and
   - **(c)** has been instructed by FF in the requirements relevant to the performance of the obligations of FF under these Clauses, in particular the limited purpose of the data processing.
3. **Copy Control.** FF shall not make copies of Personal Data, provided, however, that FF may retain copies of Personal Data provided to it for backup and archive purposes.
4. **Security Controls.** The Service includes a variety of configurable security controls that allow the Customer to tailor the security of the Service 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 passwords are stored using a one-way hashing algorithm (SHA-256) and are never transmitted unencrypted.
   - 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, FF 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.
   - Processor's 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.** FF, 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, which are encrypted via SSL while in transmission. 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.** FF shall ensure that all FF 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.** FF maintains security incident management policies and procedures. FF will promptly notify Customer in the event FF becomes aware of an actual or reasonably suspected unauthorised disclosure of Personal Data.
10. **Physical Security.** FF'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, SSL accelerators, load balancers, Web servers and application servers that are part of the 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.** FF 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. FF 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.** FF plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. FF 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

- Financials (Accounting)
- Supply Chain Management
- Service Contracts
- Revenue Recognition
- Billing
- Professional Services Automation (PSA)
- Human Capital Management
- Financial Management Community
- PSA Community