DATA PROCESSING ADDENDUM

(*Revision May 2025*)

This Data Processing Addendum, including its Schedules, ("DPA") forms part of the Main Services Agreement or other written or electronic agreement between SFDC and Customer for the purchase of online services (including associated SFDC offline or mobile components) from SFDC (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.

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

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1 and 2.
2. This DPA has been pre-signed on behalf of SFDC. Schedule 2, section 1 has been pre-signed by Salesforce, Inc. as the data importer. Please note that the contracting entity under the Agreement may be a different entity to Salesforce, Inc.
3. To complete this DPA, Customer must:
   a. Complete the information in the signature box and sign on page .
   b. Send the signed DPA to SFDC by email to dataprocessingaddendum@salesforce.com indicating, if applicable, the Customer's Account Number (as set out on the applicable SFDC Order Form or invoice).

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by SFDC of the validly completed DPA at this email address.

For the avoidance of doubt, signature of the DPA on page 8 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendix, Customer should also complete the information as the data exporter and sign on page 14 (Schedule 2).

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 SFDC 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 SFDC 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 Form(s), and the SFDC entity that is party to such Order Form is party to this DPA. For the purposes of this DPA, any reference to Order Form herein shall include "Ordering Document" (as defined in the Agreement).

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 who is a party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor an Agreement directly with SFDC, but is instead a customer indirectly via an authorized reseller of Salesforce services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

DATA PROCESSING TERMS

1. DEFINITIONS

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

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

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act, and its implementing regulations.

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

"**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and its Authorized Affiliates.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data", provided that such data is electronic data and information submitted by or for Customer to the Services. This DPA does not apply to Content or Non-SFDC Applications as defined in the Agreement or, if not defined in the Agreement, as defined in the Main Services Agreement at https://www.salesforce.com/company/legal/agreements/.

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

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

"**Europe**" means the European Union, the European Economic Area, Switzerland and the United Kingdom.

"**GDPR**" means 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), including as implemented or adopted under the laws of the United Kingdom.

"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" or **"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"Salesforce Processor BCR" means Salesforce's processor binding corporate rules for the Processing of Personal Data, the most current versions of which are available on SFDC's website, currently located at https://www.salesforce.com/company/privacy.

"Security, Privacy and Architecture Documentation" means the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via SFDC's Trust and Compliance webpage at https://www.salesforce.com/company/legal/trust-and-compliance-documentation/ (also accessible via http://www.salesforce.com/company/legal/agreements/ under the "Trust and Compliance Documentation" link), or as otherwise made reasonably available by SFDC.

"SFDC" means the SFDC entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being Salesforce, Inc. (f/k/a salesforce.com, inc.), a company incorporated in Delaware, US; Salesforce.com Canada Corporation, a company incorporated in Canada; salesforce.com France, a French S.A.S company with a share capital of 37,000 €, registered with the Paris Trade Registry under number 483 993 226 RCS Paris, Registered office: 3 Avenue Octave Gréard, 75007 Paris, France; salesforce.com Germany GmbH, a limited liability company, incorporated in Germany; Salesforce.com Italy S.r.l., an Italian limited liability company having its registered address at Piazza Filippo Meda 5, 20121 Milan (MI), VAT / Fiscal code n. 04959160963; Salesforce Systems Spain, S.L., a limited liability company incorporated in Spain; Salesforce UK Limited (f/k/a salesforce.com EMEA Limited), a company registered in England and Wales; SFDC Ireland Limited, a limited liability company incorporated in Ireland; Salesforce Japan Co., LTD (f/k/a Kabushiki Kaisha salesforce.com), a company incorporated in Japan ; Salesforce.com Singapore Pte. Ltd., a company incorporated in Singapore; SFDC Australia Pty, Ltd., a company incorporated in New South Wales; Salesforce.com India Private Limited, an Indian private limited company; Salesforce.org, LLC, a company registered in California, US; Salesforce.org EMEA Limited, a private company, limited by shares, registered in England and Wales; Salesforce Tecnologia Ltda., a limited

liability company incorporated in Brazil,, US; Demandware, LLC, a company registered in Delaware, US;, Heroku, Inc., a company incorporated in Delaware, US; Krux Digital, LLC, a company registered in Delaware, US; MuleSoft, LLC, a company registered in Delaware, US; Tableau Software, LLC, a company registered in Delaware, US; Tableau International, Unlimited Company, a company incorporated in Ireland; Vlocity, LLC, a company registered in Delaware, US; Slack Technologies, LLC, a limited liability company formed in Delaware, US; Slack Technologies Limited, a private company limited by shares incorporated under the laws of Ireland; or as applicable.

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

"Standard Contractual Clauses" means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

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

2. PROCESSING OF PERSONAL DATA

2.1. **Customer's Processing of Personal Data.** Customer as Controller or Processor shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of SFDC as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). 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. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.

2.2. **SFDC's Processing of Personal Data.** SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented 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 documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.3. **Details of the Processing.** The subject-matter of Processing of Personal Data by SFDC 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 2 (Description of Processing/Transfer) to this DPA.

2.4. **Customer Instructions**. SFDC shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if SFDC is unable to follow Customer's instructions for the Processing of Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Request.** SFDC shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". SFDC shall not respond to a Data Subject Request itself, except that Customer authorizes SFDC to redirect the Data Subject Request as necessary to allow Customer to respond directly.

3.2. **Required Assistance.** Taking into account the nature of the Processing, SFDC shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3. **Additional Assistance.** To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SFDC shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SFDC is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from SFDC's provision of such assistance.

4. SFDC PERSONNEL AND DATA PROTECTION OFFICER

4.1. **Confidentiality, Reliability and Limitation of Access.** SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. SFDC shall

(i) ensure that such confidentiality obligations survive the termination of the personnel engagement;

(ii) take commercially reasonable steps to ensure the reliability of any SFDC personnel engaged in the Processing of Personal Data; and

(iii) ensure that SFDC's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement, any applicable Order Form(s) and Documentation.

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

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) SFDC's Affiliates may be retained as Sub-processors; and (b) SFDC and SFDC's Affiliates respectively may engage third-party Sub-processors to provide the Services. SFDC or an SFDC Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. **Current List of Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under the Infrastructure and Sub-processor Documentation which can be found on SFDC's Trust and Compliance webpage at https://www.salesforce.com/company/legal/trust-and-compliance-documentation/ ("Infrastructure and Sub-processor Documentation", also accessible via http://www.salesforce.com/company/legal/agreements/ under the "Trust and Compliance Documentation" link). Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. The Infrastructure and Sub-processor Documentation contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Customer subscribes, SFDC shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data to provide the applicable Services.

5.3. **Objection Right for New Sub-processors.** Customer may object to SFDC's use of a new Sub-processor by notifying SFDC promptly in writing within thirty (30) days of receipt of SFDC's notice in accordance with the mechanism set out in section 5.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, SFDC 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 Customer. If SFDC 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) with respect only to those Services which cannot be provided by SFDC without the use of the objected-to new Sub-processor by providing written notice to SFDC. SFDC will refund 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. **Liability.** SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. SECURITY, CERTIFICATIONS AND AUDIT

6.1. **Controls for the Protection of Customer Data.** SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Documentation. SFDC regularly monitors compliance with these measures. SFDC will not materially decrease the overall security of the Services during a subscription term.

6.2. **Third-Party Certifications and Audits.** SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, SFDC agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement

6.3. **Audit Program.** SFDC shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA, including those obligations required by applicable Data Protection Laws and Regulations, as set forth in this section 6.3.

6.3.1. Access to Third-Party Certifications and Audits Information. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, SFDC shall:

(i) the make available to Customer (or Customer's Third-Party Auditor - as defined below in section 6.3.4) information regarding SFDC's compliance with the obligations set forth in this DPA in the form of a copy of SFDC's then most recent third-party audits or certifications set forth in the Security, Privacy and Architecture Documentation. Such third-party audits or certifications may also be shared with Customer's competent supervisory authority on its request;
(ii) provide Customer with a report and/or confirmation of SFDC's audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to SFDC, to the extent such reports or evidence may be shared with Customer ("Third-party Sub-processor Audit Reports"). Customer acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to SFDC may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.3.2. On-Site Audit. Customer can request an on-site audit of SFDC's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Customer either itself or through a Third-Party Auditor (as defined below in section 6.3.4) selected by Customer when:

(i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;
(ii) Customer has received a notice from SFDC of a Customer Data Incident; or
(iii) such an audit is required by Data Protection Laws and Regulations or by Customer's competent supervisory authority.

Any On-Site Audits will be limited to Customer Data Processing and storage facilities operated by SFDC or any of SFDC's Affiliates.

6.3.3. Reasonable Exercise of Rights. An On-Site Audit shall be conducted by Customer or its Third-Party Auditor:

(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Customer;
(ii) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter notice period, SFDC will use good faith efforts to accommodate the On-Site Audit request; and
(iii) during SFDC's normal business hours, under reasonable duration and shall not unreasonably interfere with SFDC's day-to-day operations.

Customer acknowledges that SFDC operates a multi-tenant cloud environment. Before any On-Site Audit commences, Customer and SFDC shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of SFDC. SFDC shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other SFDC customers' information.

6.3.4. Third-Party Auditor. A Third-Party Auditor means a third-party independent contractor that is not a competitor of SFDC. An On-Site Audit can be conducted through a Third Party Auditor if:

(i) prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect SFDC's proprietary information; and
(ii) the costs of the Third-Party Auditor are at Customer's expense.

6.3.5. Findings. Customer must promptly provide SFDC with information regarding any non-compliance discovered during the course of an On-Site Audit.

6.4. **Data Protection Impact Assessment.** Upon Customer's request, SFDC shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Data Protection Laws and Regulations 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 SFDC.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

SFDC maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and shall notify Customer without undue delay after becoming aware of the accidental or unlawful

destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by SFDC or its Sub-processors of which SFDC becomes aware (a "Customer Data Incident"). SFDC shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as SFDC deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within SFDC's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. GOVERNMENT REQUESTS

8.1 SFDC requirements. As a Processor, SFDC shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If SFDC receives a legally binding request to access Personal Data from a Public Authority, SFDC shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent SFDC is prohibited by law from providing such notification, SFDC shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable SFDC to communicate as much information as possible, without undue delay. Further, SFDC shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. SFDC shall pursue appeals where available. When challenging a request, SFDC shall seek interim measures to suspend the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. SFDC agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. SFDC shall promptly notify Customer if SFDC becomes aware of any direct access by a Public Authority to Personal Data and provide information available to SFDC in this respect, to the extent permitted by law. SFDC certifies that SFDC (1) has not purposefully created back doors or similar programming for the purpose of allowing access to the Services and/or Personal Data by any Public Authority; (2) has not purposefully created or changed its business processes in a manner that facilitates access to the Services and/or Personal Data by any Public Authority; and (3) at the Effective Date is not currently aware of any national law or government policy requiring SFDC to create or maintain back doors, or to facilitate access to the Services and/or Personal Data, to keep in its possession any encryption keys or to hand-over the encryption key to any third party. If SFDC receives an order from a government to suspend or cease cloud operations in Europe, SFDC shall promptly contest such a measure using all legal avenues available, including by pursuing litigation in court.

8.2 Sub-processors requirements. SFDC shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses and Salesforce Processor BCR.

9. RETURN AND DELETION OF CUSTOMER DATA

SFDC 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 Security, Privacy and Architecture Documentation. Until Customer Data is deleted or returned, SFDC shall continue to comply with this DPA and its Schedules.

10. AUTHORIZED AFFILIATES

10.1. **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between SFDC and each such Authorized Affiliate subject to the provisions of the Agreement and this section 10 and section 11. 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 a party only to this DPA. All access to and use of the Services and Content 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.

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

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

10.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against SFDC 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 itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).

10.3.2 The parties agree that 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 SFDC and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. 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 SFDC, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section 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, SFDC's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the 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.

12. EUROPE SPECIFIC PROVISIONS

12.1. **Definitions.** For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:

"European Personal Data" means the Personal Data subject to European Data Protection Laws and Regulations.

"**European Data Protection Laws and Regulations**" means the Data Protection Laws and Regulations applying in Europe.

"SCC Module 2" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

"SCC Module 3" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

"**Third-Country Transfer**" means a transfer of European Personal Data that is not subject to an adequacy decision by the European Commission. When US entities part of the SFDC Group or its Sub-processors are certified under the EU-US Data Privacy Framework and its extensions, the Parties agree that transfers to such entities are not considered Third-Country Transfers.

12.2. **GDPR.** SFDC will Process Personal Data in accordance with the GDPR requirements directly applicable to SFDC's provision of its Services.

12.3. **Transfer mechanisms for data transfers.** If, in the performance or use of the Services, European Personal Data is subject to a Third-Country Transfer, the transfer mechanisms listed below shall apply:

- **Salesforce Processor BCR**, which shall apply to the Services listed in the Appendix to the Salesforce Processor BCR (the "BCR Services"), subject to the additional terms in section 1 of Schedule 1;
- **SCC Module 2**. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter , subject to the additional terms in section 2 of Schedule 1; and/or
- **SCC Module 3**. Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter , subject to the additional terms in sections 2 and 3 of Schedule 1.

12.4. **Impact of local laws**. As of the Effective Date, SFDC has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent SFDC from fulfilling its obligations under this DPA. If SFDC reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, SFDC shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If SFDC is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by SFDC in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

13. APEC PRIVACY RECOGNITION FOR PROCESSORS

SFDC and the SFDC Group have obtained APEC Privacy Recognition for Processors ("PRP") certification and shall Process Personal Data submitted to the Services listed in Salesforce's PRP Notice, which SFDC makes available online at https://www.salesforce.com/company/privacy/, in accordance with this certification. Notwithstanding the foregoing, Slack Technologies, LLC and Slack Technologies Limited (collectively "**Slack**") have obtained PRP certification and shall Process Personal Data submitted to Services provided by Slack in accordance with this certification, which is available online at https://slack.com/trust/security.

14. LEGAL EFFECT

This DPA shall only become legally binding between Customer and SFDC (and Salesforce, 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: Transfer Mechanisms for European Data Transfers
Schedule 2: Description of Processing/Transfer

The parties' authorized signatories have duly executed this DPA:

CUSTOMER

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

SALESFORCE, INC. (F/K/A SALESFORCE.COM, INC.)

Signature: DocuSigned by: Lindsey Finch AC1D6EC340C1432...

Print Name: Lindsey Finch

Title: EVP, Global Privacy.

Date: June 2, 2025

SALESFORCE.COM CANADA CORPORATION

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: Vice President.

Date: June 2, 2025

SALESFORCE.COM FRANCE S.A.S.

Signature: DocuSigned by: Stephane Jaccottet D14522FE1DEE454...

Print Name: Stéphane Jaccottet

Title: President

Date: June 2, 2025

SALESFORCE.COM GERMANY GMBH

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Managing Director

Date: June 2, 2025

SALESFORCE.COM INDIA PRIVATE LIMITED

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SALESFORCE.COM ITALY S.R.L.

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SALESFORCE.COM SINGAPORE PTE. LTD.

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SALESFORCE JAPAN CO., LTD. (F/K/A KABUSHIKI KAISHA SALESFORCE.COM)

Signature: DocuSigned by: E63357C52F97482...

Print Name: Shinichi Koide

Title: Chairman

Date: June 2, 2025

SALESFORCE SYSTEMS SPAIN, S.L.

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SALESFORCE TECNOLOGIA LTDA.

Signature: DocuSigned by: D8AE75BDE7D7447...

Print Name: Alexandre Costa

Title: Manager.

Date: June 2, 2025

SALESFORCE UK LIMITED (F/K/A SALESFORCE.COM EMEA LIMITED)

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SFDC AUSTRALIA PTY, LTD.

Signature: Signed by: 80DACCF756BA43E...

Print Name: Joachim Wettermark

Title: Director.

Date: June 2, 2025

SFDC IRELAND LIMITED

Signature: DocuSigned by: 8A5F90DBE8F6408...

Print Name: Darryl Yee

Title: Director

Date: June 2, 2025

DEMANDWARE, LLC

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

HEROKU, INC.

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

MULESOFT, LLC

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

SLACK TECHNOLOGIES LIMITED

Signature: DocuSigned by: Patrick Tobin 51B81B85D7D64B7...

Print Name: Patrick Tobin

Title: Director

Date: June 2, 2025

SLACK TECHNOLOGIES, LLC

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

TABLEAU SOFTWARE, LLC

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

VLOCITY, LLC

Signature: DocuSigned by: A87B0CFD57C5474...

Print Name: Scott Siamas

Title: President and Secretary

Date: June 2, 2025

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. ADDITIONAL TERMS FOR BCR SERVICES

1.1. **Instructions and Notices.** Where Customer acts as a Processor under the instructions of the relevant Controller of Personal Data, Customer acknowledges and accepts that the commitments contained in the Salesforce Processor BCR are for the benefit of the ultimate Controller. Customer shall be responsible for ensuring that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to SFDC for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall also be solely responsible for forwarding any notifications received from SFDC to the relevant Controller where appropriate.

1.2. **Audits of the BCR Services**. The Parties agree that the audits of BCR Services described in the BCR shall be carried out in accordance with section 6.3 of the DPA.

1.3. **Reference to the Salesforce Processor BCR**. All provisions contained in the Salesforce Processor BCR, the most current versions which are available on SFDC's website, currently located at https://www.salesforce.com/company/privacy are incorporated by reference and are an integral part of this DPA.

1.4. **Liability**. In accordance with the Agreement, Customer shall have the right to enforce the Salesforce Processor BCR against the SFDC Group, including judicial remedies and the right to receive compensation.

1.5. **Conflict**. In the event of any conflict or inconsistency between this DPA and the Salesforce Processor BCR, the Salesforce Processor BCR shall prevail.

2. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

For the purposes of SCC Module 2 and SCC Module 3, Customer is the data exporter and Salesforce, Inc. ("SFDC Inc") is the data importer and the Parties agree to the following. Where the SFDC entity that is a party to this DPA is not SFDC Inc, that SFDC entity is carrying out the obligations of the data importer on behalf of SFDC Inc. If and to the extent an Authorized Affiliate relies on SCC Module 2 or SCC Module 3 for the transfer of Personal Data, any references to 'Customer' in this Schedule, include such Authorized Affiliate. Where this section 2 does not explicitly mention SCC Module 2 or SCC Module 3 it applies to both of them.

2.1. **Reference to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

2.2. **Docking clause.** The option under clause 7 shall not apply.

2.3. **Instructions.** This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to SFDC for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.2 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

2.4. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by SFDC to Customer only upon Customer's written request.

2.5. **Security of Processing.** For the purposes of clause 8.6(a), Customer is responsible for making an independent determination as to whether the technical and organizational measures set forth in the Security, Privacy and Architecture Documentation meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by SFDC provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Incident Management and Notification) of this DPA.

2.6. **Audits of the SCCs.** The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.3 of this DPA.

2.7. **General authorization for use of Sub-processors.** Option 2 under clause 9 shall apply. For the purposes of clause 9(a), SFDC has Customer's general authorization to engage Sub-processors in accordance with section 5 of this DPA. SFDC shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA.

2.8. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to clause 9(a), Customer acknowledges and expressly agrees that SFDC may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. SFDC shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

2.9. **Complaints - Redress.** For the purposes of clause 11, and subject to section 3 of this DPA, SFDC shall inform data subjects on its website of a contact point authorized to handle complaints. SFDC shall inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. SFDC shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

2.10. **Supervision.** Clause 13 shall apply as follows:

2.10.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2.10.2. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

2.10.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as competent supervisory authority.

2.10.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws and Regulations"), the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

2.10.5. Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws and Regulations"), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

2.11. **Notification of Government Access Requests.** For the purposes of clause 15(1)(a), SFDC shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

2.12. **Governing Law.** The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of France; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales..

2.13. **Choice of Forum and Jurisdiction.** The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) France; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the courts of England and Wales shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

2.14. **Appendix.** The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

2.15. **Data Exports from the United Kingdom under the Standard Contractual Clauses.** For data transfers governed by UK Data Protection Laws and Regulations, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 2 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

2.16. **Data Exports from Switzerland under the Standard Contractual Clauses.** For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws

until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

2.17. **Conflict.** The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

3. ADDITIONAL TERMS FOR SCC MODULE 3

For the purposes of SCC Module 3 (only), the Parties agree the following.

3.1. **Instructions and notifications.** For the purposes of clause 8.1(a), Customer hereby informs SFDC that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to SFDC for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from SFDC to the relevant Controller where appropriate.

3.2. **Security of Processing.** For the purposes of clause 8.6(c) and (d), SFDC shall provide notification of a personal data breach concerning Personal Data Processed by SFDC to Customer.

3.3. **Documentation and Compliance.** For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to SFDC by Customer. If SFDC receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

3.4. **Data Subject Rights**. For the purposes of clause 10 and subject to section 3 of this DPA, SFDC shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2 - DESCRIPTION OF PROCESSING/TRANSFER

1. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name: Customer and its Authorized Affiliates.

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date:

Role: For the purposes of SCC Module 2 Customer and/or its Authorized Affiliate is a Controller. For the purposes of SCC Module 3 Customer and/or its Authorized Affiliate is a Processor.

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: Salesforce, Inc.

Address: Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA

Contact person's name, position and contact details: Lindsey Finch, DPO, privacy@salesforce.com

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date: DocuSigned by: Lindsey Finch AC1D6EC340C1432...

7/31/2025

Role: Processor

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

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:

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

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

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
- Personal life data
- Localisation data

4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Customer may submit special categories of data to the Services, the extent of which is determined and controlled by Customer 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, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The applicable security measures are described under the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via SFDC's Trust and Compliance webpage at https://www.salesforce.com/company/legal/trust-and-compliance-documentation/ (also accessible via http://www.salesforce.com/company/legal/agreements/ under the "Trust and Compliance Documentation" link), or as otherwise made reasonably available by SFDC.

5. FREQUENCY OF THE TRANSFER

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
Continuous basis depending on the use of the Services by Customer.

6. NATURE OF THE PROCESSING

The nature of the Processing is the performance of the Services pursuant to the Agreement.

7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

SFDC 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.

8. DURATION OF PROCESSING

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Subject to section 9 of the DPA, SFDC will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

9. SUB-PROCESSOR TRANSFERS

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed under the Infrastructure and Sub-processor Documentation which can be found on SFDC's Trust and Compliance webpage (also accessible via http://www.salesforce.com/company/legal/agreements/ under the "Trust and Compliance Documentation" link).

10. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13: the supervisory authority specified in section 2.10 of Schedule 1 shall act as the competent supervisory authority.

11. TECHNICAL AND ORGANISATIONAL MEASURES

SFDC will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Customer. SFDC will not materially decrease the overall security of the Services during a subscription term.