SUPPLIER PRIVACY EXHIBIT

(*March 2024*)

This Supplier Privacy Exhibit ("**Privacy Exhibit**") forms part of the Agreement to which it is attached, where it is included by reference or where it forms an exhibit to such Agreement, as applicable. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. Any section or schedule referenced in this Privacy Exhibit shall refer to sections and schedules in this Privacy Exhibit only. In the event of any conflict or inconsistency between the Privacy Exhibit and the Agreement, the Privacy Exhibit will prevail unless stated otherwise in this Privacy Exhibit.

In the course of providing Services to Salesforce, Supplier may Process: (i) Personal Data; (ii) Salesforce Customer Data; and (iii) Salesforce Data as a Processor and the Parties agree to comply with the following provisions, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

"**Agreement**" means for the purposes of this Privacy Exhibit, any and all agreements between Salesforce or Salesforce Group and Supplier and/or its Affiliates (including addendums, attachment, exhibits or child agreements including but not limited to Statements of Works and Order Forms) resulting in Supplier Processing: (i) Personal Data; (ii) Salesforce Customer Data; and/or (iii) Salesforce Data.

"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.

"Data Protection Laws and Regulations" means all laws and regulations, including but not limited to those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"Data Subject" means the identified or identifiable person to whom Personal Data relates. "Data Subject" shall be understood to include "Consumer" and analogous terms under applicable Data Protection Laws and Regulations.

"**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 Processed by Supplier under the Agreement relating to: (i) an identified or identifiable natural person; (ii) an identified or identifiable household (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations); and/or (iii) 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).

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

"**Salesforce Customer(s)**" means: (i) a legal entity with whom a member of the Salesforce Group has entered into a contract to provide Salesforce products and services, including professional services; or (ii) a legal entity with whom a member of the Salesforce Group has executed a contract under which the legal entity is entitled to resell Salesforce's products and services to its end customers.

"**Salesforce Customer Data**" means any electronic data and information, including but not limited to Personal Data: (i) submitted to Supplier by or for Salesforce Customer; (ii) accessed by Supplier for provision of the Services to Salesforce

Customer; or (iii) generated by Salesforce Customer's use of Salesforce's products and services.

"Salesforce Data" means any electronic data and information, which is not Salesforce Customer Data, including but not limited to Personal Data: (i) submitted to Supplier by or for Salesforce; (ii) accessed by Supplier for provision of the Services to Salesforce; or (iii) generated by Salesforce's use of the Services.

"Salesforce Group" means Salesforce and its Affiliates.

"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 Supplier to provide the Services.

"Supervisory Authority" means any local, national, supranational, state, governmental or quasi-governmental agency, body, department, board, official or entity exercising regulatory or supervisory authority pursuant to any Data Protection Laws and Regulations in accordance with this Agreement.

"UK Addendum" means the UK Addendum to the Standard Contractual Clauses (Version B1.0), as at 15 July 2022 set out at international-data-transfer-addendum.pdf (ico.org.uk).

2. PROCESSING OF PERSONAL DATA

2.1. **Supplier's Processing of Personal Data.** Supplier shall act only as a Processor and shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. If and to the extent that Supplier determines that it can no longer meet its obligations under such Data Protection Laws and Regulations, Supplier shall inform Salesforce in writing immediately. Supplier shall Process Personal Data on behalf of and only in accordance with Salesforce's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; and (ii) Processing to comply with other documented instructions provided by Salesforce where such instructions are consistent with the Agreement. Supplier hereby certifies that it will not collect, retain, use, disclose, share, sell or otherwise Process Personal Data: (i) for any other purposes, including retaining, using, disclosing, sharing, selling or otherwise Processing Personal Data for a commercial purpose other than providing the Services; or (ii) outside of the direct business relationship between Salesforce and Supplier. Supplier shall not combine Personal Data received from or on behalf of Salesforce with other Personal Data, except as required to achieve a "business purpose," as that term is defined in the CCPA. If Supplier processes de-identified data on Salesforce's behalf, Supplier shall: (i) commit to continue to maintain and use de-identified data in a de-identified form and not attempt to re-identify the de-identified data; and (ii) contractually obligate any recipients of the de-identified data to comply with Data Protection Laws and Regulations.

2.2. **Details of the Processing.** The subject matter of Processing of Personal Data by Supplier 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 Privacy Exhibit are further specified in Schedule 2 (Description of Processing/Transfer).

2.3. **Records of Processing.** Upon Salesforce's request, Supplier shall provide cooperation and assistance compiling or maintaining Salesforce's records of Processing as required by Data Protection Laws and Regulations.

3. PROCESSING OF SALESFORCE CUSTOMER DATA

To the extent Supplier, when providing its Services, Processes Salesforce Customer Data, Supplier is a sub-processor of Salesforce and subject to the provisions in this Section 3 (Processing of Salesforce Customer Data):

3.1. **Rights of Salesforce Customers.** The Parties acknowledge and agree that Salesforce Customers, if and to the extent required under applicable Data Protection Laws and Regulations, shall be entitled to exercise the rights and seek remedies under: Sections 2.2 (Details of the Processing); 2.3 (Record of Processing); 4 (Rights of Data Subject); 6 (Sub-Processors); 7.2 (Audit Program); 7.3 (Data Protection Impact Assessment); 8 (Personal Data Incident Management and Notification) and 10 (Return and Deletion of Personal Data) of this Privacy Exhibit, subject to the terms of this Section 3 (Processing of Salesforce Customer Data).

3.1.1 Instructions; Supplier's Processing of Personal Data. In addition to Section 2.2 (Details of the Processing), Supplier acknowledges that: (i) Salesforce communicates Processing instructions on behalf of Salesforce Customers; and (ii) Salesforce Customers may issue additional instructions.

3.1.2 Sub-Processors. Supplier's obligations under Section 6 (Sub-Processors) regarding the appointment of Sub-processors shall apply with respect to Salesforce Customers, including but not limited to Salesforce Customers' right to object to a new Sub-Processor, to request a copy of Sub-processor agreement and to request an updated list of Supplier's Sub-Processors. To the extent possible and reasonable, Salesforce will exercise such rights on behalf of Salesforce Customers. If Salesforce requests a copy of a Sub-processor agreement from Supplier under Section 6.5 (Copies of Sub-processing Agreements), Supplier acknowledges and agrees that Salesforce may share such agreements with applicable Salesforce Customers.

3.1.3 Audits. To the extent required under applicable Data Protection Laws and Regulations, Salesforce Customers and their regulators shall have the same rights and obligations as Salesforce with regard to on-site audits of Supplier (and Supplier's Sub-processors') security and data protection measures, architecture, systems, policies and procedures relevant to the Processing of Salesforce Customer Data, under Section 7.2 (Audit) In addition to Section 7.2.1 (Certifications and Audits), Salesforce Customers shall have an audit right under Section 7.2 (Audit) to verify compliance with the data protection controls set forth in the Salesforce Processor BCR. If Salesforce requests an audit report from Supplier under Section 7.2.5 (Audit Results), Supplier acknowledges and agrees that upon written request from a Salesforce Customer, Salesforce may provide the requesting Salesforce Customer copies of any audit reports.

3.1.4 Salesforce Customer Data Incident Management and Notification. Supplier's obligation under Section 8 (Personal Data Incident and Management and Notification) to provide assistance to Salesforce in the context of a Personal Data Incident shall include providing information required for Salesforce Customers' notification obligations as required by Data Protection Laws and Regulations.

3.1.5 Return of Salesforce Customer Data. To the extent required to fulfill Salesforce's or Salesforce Customers' obligations under Data Protection Laws and Regulations, Supplier shall extend the rights in Section 10 (Return and Deletion of Personal Data) with respect to Salesforce Customer Data to Salesforce Customers and their regulators. To the extent reasonably possible Salesforce shall exercise such rights on behalf of Salesforce Customers.

3.1.5 Assistance. Upon request, Supplier shall: (i) make available to Salesforce Customers all information necessary to demonstrate compliance with this Privacy Exhibit and applicable Data Protection Laws and Regulations; (ii) provide cooperation and assistance with compiling or maintaining Salesforce Customers' records of Processing as required by Data Protection Laws and Regulations, whereby Supplier acknowledges that Salesforce Customers may be required, upon its supervisory authority request, to make such records available to the supervisory authorities; and (iii) provide Salesforce Customers with reasonable cooperation and assistance as needed.

3.2. **Salesforce Processor BCR.** Supplier acknowledges that the Salesforce Processor BCR is relied upon as a legal transfer mechanism between Salesforce Customers and Salesforce to cover transfers of Salesforce Customer Data. Supplier agrees that it shall abide by all the terms imposed on Salesforce's sub-processors under the most current versions of the Salesforce Processor BCR regarding such Personal Data. In case of any conflict between this Privacy Exhibit and the applicable terms of the Salesforce Processor BCR, the Salesforce Processor BCR shall prevail.

4. RIGHTS OF DATA SUBJECTS

4.1. **Data Subject Request.** Supplier shall, to the extent legally permitted, promptly notify Salesforce in writing at privacy@salesforce.com 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." Supplier shall not respond to a Data Subject Request itself, except that Salesforce authorizes Supplier to redirect the Data Subject Request as necessary to allow Salesforce to respond directly.

4.2. **Required Assistance.** Taking into account the nature of the Processing, Supplier shall assist Salesforce by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Salesforce's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. Supplier shall upon Salesforce's request use commercially reasonable efforts to assist Salesforce in responding to such Data Subject Request, to the extent Supplier is legally permitted to do so.

5. SUPPLIER PERSONNEL

5.1. **Confidentiality, Reliability, Limitation of Access.** Supplier 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. Supplier shall:

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

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

(iii) ensure that Supplier's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

6. SUB-PROCESSORS

6.1. **List of authorized Sub-processors and notification of new Sub-processors**. The list of Supplier's authorized Sub-processors and relevant Sub-processing details, as of the effective date of this Privacy Exhibit, is set out in the Data Processing Exhibit appended to the Agreement. Supplier shall provide 120 days' prior written notification to Salesforce at privacy@salesforce.com before permitting any new Sub-processor to Process Personal Data and/or any change of location

of Processing for any existing authorized Sub-processor. Such notification shall include the proposed Sub-processor's entity name (if it is a new Sub-processor) and all other information required in the Data Processing Exhibit. If Salesforce does not object to the new Sub-processor or change of location of Processing for an existing Sub-processor (as applicable) within 120 days after receiving that notification, subject to the terms of the Agreement and this Privacy Exhibit, then the update shall be considered effective. Supplier shall make the latest updated version of Data Processing Exhibit available to Salesforce upon its request.

6.2. **Objection Right.** If Salesforce objects to a new Sub-processor and/or any change of location of Processing for an existing Sub-processor, Supplier will make available to Salesforce a change in the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If Supplier is unable to make available such change within thirty (30) days of Salesforce's objection, Salesforce may terminate those Services which cannot be provided by Supplier without the use of the objected-to new Sub-processor by providing written notice to Supplier. Supplier will refund Salesforce any prepaid fees covering the remainder of the Services following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Salesforce, and Supplier shall ensure that the objected-to new Sub-processor does not Process Personal Data.

6.3. **Requirements for the use of Sub-processors.** Supplier's use of Sub-processors shall be subject to the following:

a. Supplier shall be fully responsible for the performance of any Sub-processor and their compliance with all obligations applicable to the Processing of Personal Data, Salesforce Customer Data, and Salesforce Data and with Data Protection Laws and Regulations. Supplier shall conduct proper due diligence on all Sub-processors to ensure each Sub-processor can comply with Data Protection Laws and Regulations, all applicable terms and conditions of the Agreement and all applicable Salesforce policies and procedures to which Supplier may be subject during the term of the Agreement.
b. Sub-processors retained by Supplier shall at all times be deemed Sub-processors of Supplier and shall not under any circumstance be construed or deemed to be employees or Sub-processors of Salesforce.

6.4. **Sub-processing Agreements.** Supplier shall ensure that it has a written contract in place with the relevant Sub-processor that contains data protection obligations no less restrictive than those set out in this Privacy Exhibit.

6.5. **Copies of Sub-processing Agreements.** Upon Salesforce's request, Supplier shall provide Salesforce with copies of any sub-processing agreements it has entered into in connection with the Services. Supplier shall provide such copies to Salesforce within ten (10) days of Salesforce's request. Supplier may remove any commercial information from such copies before providing them to Salesforce.

7. SECURITY, CERTIFICATIONS, AND AUDITS

7.1. **Controls for the Protection of Salesforce Customer Data and Salesforce Data.** Taking into account the principle of data protection by design and by default, Supplier hereby certifies that it maintains appropriate technical and organizational measures for protection of the security of Salesforce Customer Data and Salesforce Data, including protection against: (i) unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Salesforce Customer Data and Salesforce Data; and (ii) retaining, using, disclosing, selling or otherwise Processing Salesforce Customer Data and Salesforce Data. Supplier will not decrease the overall security of the Services.

7.2. **Audit Program.** Supplier shall maintain an audit program to help ensure compliance with the obligations set out in this Privacy Exhibit and shall make available to Salesforce information to demonstrate compliance with the obligations set out in this Privacy Exhibit and in Data Protection Laws and Regulations, as set forth in this Section 7.2 (Audit Program).

7.2.1 Certifications and Audits. Supplier shall meet the following certification obligations and maintain these certifications and reports or successors:

a. Subject to reasonable confidentiality obligations consistent with generally accepted industry practices regarding the report, once per year during the term of the Agreement Supplier shall, upon request, provide Salesforce with an SSAE 18 SOC 2, Type 2 Report and all other third party reports relating to Supplier's information security obligations herein; and
b. Supplier operates an information security management system ("ISMS") for the Services in accordance with the ISO 27001 international standard. Supplier has achieved ISO 27001 certification for its ISMS from an independent third party. Supplier's ISO 27001 Certificate and Statement of Applicability shall be made available to Salesforce upon request.

7.2.2 Right to Audit. In addition to any other audit rights described in the Agreement, Salesforce and its regulators shall have the right to an on-site audit of Supplier's (and Supplier's Sub-processors') Processing activities covered by this Privacy Exhibit as follows:

a. Following any notice from Supplier to Salesforce of a Personal Data Incident (as defined in Section 8 (Personal Data Incident Management and Notification) below);

b. Upon Salesforce's reasonable belief that Supplier is not in compliance with its data protection obligations;
c. To verify whether Personal Data was disclosed to a Public Authority and under which conditions, to assess if Personal Data was disclosed beyond what is necessary and proportionate in a democratic society;
d. As required by law or regulators;
e. For any other reason, once annually.

7.2.3 Audit Terms. Any audits described in Section 7.2 (Audit Program) shall be conducted:
a. By Salesforce or its regulators and/or Salesforce Customer or its regulators, or through a third party, independent contractor selected by one of those parties;
b. During reasonable times;
c. To the extent possible, upon reasonable advance notice to Supplier; and
d. Within a reasonable duration and shall not unreasonably interfere with Supplier's day-to-day operations.

7.2.4 Third Parties. If Salesforce or its regulators and/or Salesforce Customer or its regulators conduct an audit through a third party independent auditor or a third party accompanies any of the foregoing parties or participates in such audit, Salesforce will use reasonable efforts to cause such third party to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Supplier's and Supplier's customers' confidential and proprietary information.

7.2.5 Audit Results. After conducting an audit, Salesforce may notify Supplier of the manner in which Supplier does not comply with any of the applicable security, confidentiality or privacy obligations herein. Upon such notice, Supplier shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Salesforce when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Salesforce, Salesforce Customer, or the applicable regulator may conduct a follow-up audit within six (6) months of Supplier's notice of completion of any necessary changes. To the extent that an audit identifies any material security vulnerabilities, Supplier shall remediate those vulnerabilities without undue delay but not later than fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

7.3. Data Protection Impact Assessment. Upon Salesforce's request, Supplier shall provide Salesforce with cooperation and assistance needed to fulfill Salesforce's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to the Services, to the extent: (i) Salesforce does not otherwise have access to the relevant information; and (ii) such information is available to Supplier.

8. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

In addition to any other incident management and notification obligations described in the Agreement, Supplier shall maintain security incident management policies and procedures and shall notify Salesforce without undue delay and in any event within forty-eight (48) hours after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Supplier or its Sub-processors of which Supplier becomes aware (a "**Personal Data Incident**"). Such notification shall be in writing and shall be sent to security@salesforce.com. Supplier shall make reasonable efforts to identify the cause of the Personal Data Incident and take all necessary steps to remediate the cause of the Personal Data Incident to the extent the remediation is within Supplier's reasonable control. Taking into account the nature of Processing and the information available to Supplier, upon Salesforce's request, Supplier shall provide to Salesforce all information required for Salesforce's or Salesforce Customer's notification of the Personal Data Incident, to the extent known or discoverable to Supplier, consisting of: (i) time of discovery of the Personal Data Incident; (ii) nature and scope of the Personal Data Incident; (iii) additional information for Salesforce to assess: (a) Personal Data affected by the Personal Data Incident and (b) observed and probable consequences of the Personal Data Incident for the Processing of Personal Data; (iv) measures taken or proposed by Supplier to mitigate the negative effects of the Personal Data Incident; and (v) any other information related to the Personal Data Incident as reasonably requested by Salesforce. In addition, Supplier will provide indemnification to Salesforce related to such Personal Data Incident as set forth in the Agreement.

9. GOVERNMENT ACCESS REQUESTS

Supplier 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 Supplier receives a legally binding request to access Personal Data from a Public Authority, Supplier shall, unless otherwise legally prohibited, promptly notify Salesforce and shall include in such notification a summary of the nature of the request. To the extent Supplier is prohibited by law from providing such notification, Supplier shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Supplier to communicate as much information as possible, as soon as possible. Further, Supplier shall challenge the request if, after careful assessment, it

concludes that there are reasonable grounds to consider that the request is unlawful. Supplier shall pursue possibilities of appeal. When challenging a request, Supplier shall seek interim measures with a view to suspending 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. Supplier shall provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Supplier shall promptly notify Salesforce if Supplier becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Supplier in this respect, to the extent permitted by law. Supplier certifies that Supplier: (i) has not created back doors or similar programming for the purpose of allowing access to the Services and/or Personal Data by any Public Authority; (ii) has not created or changed its business processes in a manner that facilitates access to the Services and/or Personal Data by any Public Authority; and (iii) as of the effective date of this Privacy Exhibit is not currently aware of any national law or government policy requiring Supplier 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.

10. RETURN AND DELETION OF PERSONAL DATA

Supplier shall abide by the following with respect to deletion of Personal Data:

a. Within thirty (30) days following the Agreement's expiration or termination, or sooner if requested by Salesforce, Supplier shall securely destroy all copies of Personal Data (including any automatically created archival copies), unless otherwise required by applicable law, in which case Supplier shall inform Salesforce of such requirement;
b. Personal Data and tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method in accordance with high industry standards and practices;
c. Upon Salesforce's request, Supplier shall promptly return to Salesforce a copy of all Personal Data;
d. Upon Salesforce's request, Supplier shall provide, within thirty (30) days of Salesforce's request, a certificate of deletion/return certifying that Supplier has deleted/returned all Personal Data; and
e. If Supplier is obliged to retain Personal Data to comply with a legal obligation, Supplier will inform Salesforce in writing and continue to maintain the confidentiality and security of the Personal Data in accordance with the terms of the Agreement, including without limitation the confidentiality obligations thereunder, the terms of this Privacy Exhibit and the Security Exhibit.

11. EUROPE SPECIFIC PROVISIONS

11.1. **Scope.** To the extent GDPR applies to the Processing of Personal Data, the terms in this Section 11 (Europe Specific Provisions) apply.

11.2. **Definitions.** Capitalized terms used in this Section 11 (Europe Specific Provisions) and Schedule 1 (Standard Contractual Clauses Operational Provisions and Additional Terms) which are not otherwise defined in this Privacy Exhibit shall have the meaning set forth below:

"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 Salesforce Group or its Sub-processors are certified under the EU-US Data Privacy Framework and/or its extensions, the Parties agree that transfers to such entities are not considered Third-Country Transfers.

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

11.4. **Processing Instructions.** Supplier shall inform Salesforce in writing at privacy@salesforce.com immediately if: (i) in its opinion, an instruction from Salesforce or Salesforce Customer constitutes a breach of the GDPR; and/or (ii) Supplier is unable to follow Salesforce's or Salesforce Customer's instructions for the Processing of Personal Data.

11.5. **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:

(a) SCC Module 2. Where Salesforce is a Controller and a data exporter, subject to the additional terms in Schedule 1; and/or

(b) SCC Module 3. Where Salesforce is a Processor acting on behalf of a Controller and a data exporter, subject to the additional terms in Schedule 1 (Standard Contractual Clauses Operational Provisions and Additional Terms).

11.6. **Impact of local laws**. As of the effective date of this Privacy Exhibit, Supplier guarantees that it has no reason to believe that the laws and practices in any jurisdiction applicable to its Processing of the Personal Data, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Supplier from fulfilling its obligations under this Privacy Exhibit. If Supplier reasonably believes that any existing or future enacted or enforceable laws and practices in the jurisdiction applicable to its Processing of the Personal Data ("**Local Laws**") prevent it from fulfilling its obligations under this Privacy Exhibit, it shall promptly notify Salesforce in writing at privacy@salesforce.com. In such a case, Supplier shall make available to Salesforce a change in the Services acceptable to Salesforce or recommend a commercially reasonable change to Salesforce's configuration or use of the Services to facilitate compliance with the Local Laws. If Supplier is unable to make available either change promptly, Salesforce may terminate the applicable Agreement or relevant Services and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Supplier in accordance with the Local Laws by providing written notice to Supplier in accordance with the "Notices" section of the Agreement. Salesforce shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

List of Schedules

Schedule 1: Standard Contractual Clauses Operational Provisions and Additional Terms

Schedule 2: Description of Data Processing and Transfer Activities

The Parties' authorized signatories have duly executed this Privacy Exhibit:

SALESFORCE, INC.

Signature: DocuSigned by: Jennifer Browne D8C8BC00485845F...

Print Name: Jennifer Browne

Title: SVP, Chief Procurement Officer

Date: 3/25/2024

SCHEDULE 1 - STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

For the purposes of SCC Module 2 and SCC Module 3, Salesforce is the data exporter and Supplier is the data importer and the Parties agree to the following. Where the following provisions do not explicitly mention SCC Module 2 or SCC Module 3, they apply to both of them.

1.1. **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 Privacy Exhibit. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2 (Description of Data Processing and Transfer Activities).

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

1.3. **General Authorization for Use of Sub-processors.** Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Supplier has Salesforce's general authorization to engage Sub-processors in accordance with Section 6 (Sub-Processors) of this Privacy Exhibit. Supplier shall make available to Salesforce the current list of Sub-processors in accordance with Section 6.2 (Objection Right) of this Privacy Exhibit.

1.4. **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 the laws of: (i) France; or (ii) England and Wales where the Agreement is governed by the laws of England and Wales.

1.5. **Choice of Forum and Jurisdiction.** The courts under clause 18 shall be those designated in 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 for disputes.

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

- The contents of Section 1 (List of Parties) of Schedule 2 (Description of Data Processing and Transfer Activities) shall form Annex I.A to the Standard Contractual Clauses
- The contents of Sections 2 (Categories of Data Subject whose Personal Data is transferred) through Section 9 (Subprocessor Transfers) of Schedule 2 (Description of Data Processing and Transfer Activities) shall form Annex I.B to the Standard Contractual Clauses
- The contents of Section 10 (Competent Supervisory Activities) of Schedule 2 (Description of Data Processing and Transfer Activities) shall form Annex I.C to the Standard Contractual Clauses
- The contents of Section 11 (Technical and Organization Measures) of Schedule 2 (Description of Data Processing and Transfer Activities) shall form Annex II to the Standard Contractual Clauses.

1.7. **Data Exports from the United Kingdom under the Standard Contractual Clauses.** For data transfers governed by Data Protection Laws and Regulations of the United Kingdom, the Mandatory Clauses of the UK Addendum shall apply. The information required for Tables 1 to 3 of Part One of the UK Addendum is set out in Schedule 2 (Description of Data Processing and Transfer Activities) (as applicable). For the purposes of Table 4 of Part One of the UK Addendum, neither Party may end the UK Addendum when it changes.

1.8. **Data Exports from Switzerland under the Standard Contractual Clauses.** For data transfers governed by Data Protection Laws and Regulations of Switzerland ("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 to Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

1.9. **Conflict.** The Standard Contractual Clauses are subject to this Privacy Exhibit and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this Privacy Exhibit, unless stated otherwise. If the body of this Privacy Exhibit conflicts with the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

1.10. **Instructions and notifications.** For the purposes of clause 8.1(a) of SCC Module 3, Salesforce hereby informs Supplier that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data.

SCHEDULE 2 - DESCRIPTION OF DATA PROCESSING AND TRANSFER ACTIVITIES

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: 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 including relevant SOW(s) and/or Order Forms(s).

Signature and date: DocuSigned by: Jennifer Browne 3/25/2024 D8C8BC00485845F...

Role: For the purposes of the SCC Module 2 Salesforce and/or its Affiliate is a Controller. For the purposes of the SCC Module 3 Salesforce and/or its 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: Supplier and its Affiliates

Address: As set forth in the Notices Section of the Agreement

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 including relevant SOW(s) and/or Order Forms(s).

Signature and date:

Role: Processor

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Unless otherwise stated in the Data Processing Exhibit appended to the Agreement, Supplier acknowledges and recognizes that the following categories of Data Subjects will or might be Processed by Supplier to perform the Services whether such Personal Data is submitted by Salesforce (through Salesforce Customers, as applicable) or Salesforce Customers. Supplier shall promptly inform Salesforce in writing of any changes made to that list.

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

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

Unless otherwise stated in the Data Processing Exhibit appended to the Agreement, Supplier acknowledges and recognizes that the following categories of Personal Data will or might be Processed by Supplier to perform the Services whether such Personal Data is submitted by Salesforce (through Salesforce Customers, as applicable) or Salesforce Customers. Supplier shall promptly inform Salesforce in writing of any changes made to that list.

- Name
- Username
- Title

- Nationality
- Marital status
- Personal contact information
- Business contact information
- Professional life data
- Personal life data
- ID data
- Financial information
- Photos/videos
- Location
- Device/usage information
- Health/biometric/genetic information
- Ethnicity
- Sexual orientation
- Political, religious, or philosophical beliefs
- Trade union membership

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:

Data exporter may submit special categories of data to the 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 include 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 in the Security Exhibit.

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 Salesforce and/or Salesforce Customers, as applicable.

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

Supplier will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Salesforce and/or Salesforce Customers, as applicable, 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:

Supplier will Process Personal Data for the duration of the Agreement or where relevant, the duration of the Services or beyond according to 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 Section 7 (Purpose of Processing, the Data Transfer and Further Processing) above, Supplier will Process Personal Data as necessary to perform the Services pursuant to the Agreement. The Supplier will Process Personal Data for the duration of the Agreement or where relevant, the duration of the Services or beyond according to 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 in the Data Processing Exhibit appended to the Agreement.

10. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13:

- Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as the competent supervisory authority.
- The UK Information Commissioner's Office shall act as competent supervisory authority insofar as the relevant data transfer is governed by UK 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.

11. TECHNICAL AND ORGANIZATIONAL MEASURES

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data provided to the Services, as described in the Security Exhibit.