TABLEAU SOFTWARE PARTNER DATA PROCESSING ADDENDUM

By checking the "AGREED" box and clicking "SUBMIT", Partner agrees to be legally bound by all of the terms and conditions of this Tableau Software Partner Data Processing Addendum ("Processor Addendum"), which becomes effective as of the date the applicable Program Fee is paid in full or Partner submits this Processor Addendum if the Program Fee is not applicable. This Processor Addendum is between Partner ("you") and Tableau Software, LLC or the applicable Tableau affiliate ("Tableau"). Partner agrees that this Processor Addendum is enforceable like any written agreement signed by Partner. Partner represents and warrants that it has the right and authority to enter into this Processor Addendum. This Processor Addendum is subject to, made part of and incorporates by reference all other terms of the Agreement as defined in the Tableau Partner Network Partner Master Terms and any addenda thereto entered into by Tableau and Partner ("Agreement"). All capitalized undefined terms in this Processor Addendum shall have the meaning set forth in the Applicable Data Protection Laws (as defined below).

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.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and the California Attorney General's regulations.

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

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data. Tableau is the Data Controller under this Processor Addendum

"**Data Subject**" means the identified or identifiable natural individual person, household, or device linked to a consumer or household to whom Personal Data relates.

"Data Protection Laws and Regulations" means all laws, regulations, and legally binding requirements of any governmental authority or regulator applicable to the Processing of Personal Data under the Agreement. This includes laws and regulations of the United States, the European Union (and its member states), the European Economic Area (and the countries that form part of this), Switzerland and the United Kingdom, including but not limited to (a) the CCPA and any laws or regulations ratifying, implementing, adopting, supplementing or replacing the CCPA; (b) the GDPR and any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR (including, in the UK, the Data Protection Act 2018 and (to the extent in force) the UK GDPR as defined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019; (iii) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC) (including, in the UK, the Privacy and Electronic Communications (EC Directive) Regulations 2003); and (iv) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, as updated, amended or replaced from time to time.

"**DP Regulator**" means any governmental authority or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws and Regulations.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Partner Activities**" means the actions and activities which Tableau authorizes Partner to conduct under the Agreement, as well as the related obligations as specified under the Agreement.

"**Personal Data**" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a Data Subject that is Processed by Partner or Tableau in accordance with the Agreement and this Processor Addendum and any personal information or personal data as defined under any Data Protection Laws and Regulations. A Data Subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller. Partner is the Processor of Personal Data on behalf of Tableau, as the Controller, under this Processor Addendum.

"**Protected Information**" means (i) all Personal Data that Partner may Process in connection with the Partner Activities about Data Subjects, including Tableau customers, prospective customers, (and their respective employees and personnel), and (ii) Personal Data about Tableau employees and personnel.

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

"**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Information by the business to another business or a third party for monetary or other valuable consideration.

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

2. PRIVACY REQUIREMENTS

2.1 **Compliance with Applicable Laws.** With respect to its activities hereunder involving Protected Information, Partner hereby represents, warrants, and covenants that: (i) it is and will remain at all times during the term of the Agreement, and to the extent it Processes any Protected Information after the term of the Agreement, in compliance with all applicable Data Protection Laws and Regulations; (ii) its performance under the Agreement will not cause Tableau to be in violation of any Data Protection Laws and Regulations; and (iii) it shall maintain records of all Processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws and Regulations ("**Records**") and shall make such Records available to any DP Regulator on request.

2.2 **Written Instructions on Processing of Protected Information.** Partner shall Process Protected Information only on behalf of and in accordance with Tableau's documented written instructions. If any other Processing is required by applicable Data Protection Laws and Regulations, Partner shall inform Tableau of the legal requirement before commencing such Processing, unless providing this information to Tableau is legally prohibited. For purposes of

this section, Tableau instructs Partner to Process Protected Information for the following purposes: (i) Processing in accordance with the Agreement and (ii) Processing to comply with other documented reasonable instructions provided by Tableau (e.g., via email) where such instructions are consistent with the terms of the Agreement and Data Protection Laws and Regulations. Further details on the Partner's Processing activities under the Agreement are set out in Schedule 1 of this Processor Addendum. Partner shall immediately inform Tableau if, in its opinion, an instruction from Tableau infringes Data Protection Laws and Regulations or conflicts with this Processor Addendum.

2.3 Partner agrees to Process the Personal Data solely for the purpose(s) for which it has received or collected the Personal Data under the Agreement, as specified in Annex B to Schedule 1 hereto. Partner hereby certifies that it will not a) collect, retain, use, or disclose Personal Data (i) for any other purposes; or (ii) outside of the direct business relationship between Partner and Tableau; or b) Sell Personal Data, or cause Tableau to Sell Personal Data.

2.4 Partner shall cease Processing the Protected Information and Personal Data in the event that this Processor Addendum and/or the Agreement is terminated or otherwise expires.

2.5 **Provision of Information to Demonstrate Compliance.** Partner shall, and shall require its Sub-processors to make available to Tableau, or an auditor mandated by Tableau, upon request all information and facilities (including but not limited to the Records) necessary to demonstrate Partner's compliance with the obligations laid down in this Processor Addendum, and shall allow for and contribute to audits, including inspections, by Tableau or an auditor mandated by Tableau in relation to the Processing of Personal Data of Tableau and/or the Protected Information by or on behalf of Partner.

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

2.7 **Technical and Organizational Measures.** Partner shall implement and maintain appropriate technical and organizational measures that are no less than the measures set out in Appendix 2 to the Standard Contractual Clauses attached hereto and no less than the measures that Partner uses to protect its own similarly confidential data and information resources to ensure a level of security appropriate to that risk in order to:

(a) Protect Protected Information and Confidential Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or Processing in accordance with Data Protection Laws and Regulations, thereby taking into account the principles of privacy-by-design and privacy-by-default.

(b) Enable Tableau to meet its legal obligations to respond to requests from individuals under Data Protection Laws and Regulations in a timely manner, including but not limited to the ability of Partner to implement requests from individuals to access, rectify, amend, object to Processing, erase, not to be subject to automated decision-making including profiling, or port their Personal Data or to restrict or cease Processing of such Personal Data where Tableau instructs Partner to implement such a request. Partner shall immediately notify Tableau of any request related to Tableau made by an individual to exercise any individual right under Data Protection Laws and Regulations and shall cooperate with Tableau in executing Tableau's obligations related to such request. Partner may not reach out to the individual without Tableau's prior written consent except to confirm that the request relates to Tableau.

(c) Ensure and be able to demonstrate that Processing of Protected Information is performed in accordance with applicable Data Protection Laws and Regulations.

2.8 **Data Protection Impact Assessment.** Upon Tableau's request, Partner shall assist Tableau when Tableau carries out any data protection impact assessment related to Processing carried out with respect to Partner's Partner Activities under the Agreement and provide assistance to Tableau in Tableau's consultation with any DP Regulator regarding the Processing that is the subject of a data protection impact assessment. If Partner Processes Personal Data of Tableau's customers, then upon Tableau's request, Partner shall also provide Tableau with cooperation and assistance needed to fulfil Tableau's obligation to assist Tableau's customers in ensuring compliance with their obligation to carry out a data protection impact assessment or consult with DP Regulators regarding Processing that is the subject of a data protection impact assessment, including by providing all relevant information, to the extent Tableau does not otherwise have access to the relevant information needed by Tableau's customers and to the extent such information is available to Partner.

2.9 **Records of Processing.** Upon Tableau's request, Partner shall provide cooperation and assistance compiling or maintaining Tableau's records of processing as required by Data Protection Laws and Regulations. Partner acknowledges that Tableau may be required, upon its DP Regulator's request, to make such records available to the DP regulator.

2.10 **Data Subject Rights.** Partner will assist Tableau by implementing appropriate technical and organizational measures to enable Partner to fulfil Tableau's obligations in responding to requests to exercise a Data Subject's rights under the Data Protection Laws and Regulations. In particular, Partner will promptly notify Tableau without undue delay if Partner receives a request from a Data Subject under any Data Protection Laws and Regulations with respect to Personal Data; and ensure that Partner does not respond to such request except on the documented instructions of Tableau or as required by applicable Data Protection Laws and Regulations to which Partner is subject, in which case Partner shall to the extent permitted by applicable Data Protection Laws and Regulations inform Tableau of that legal requirement before Partner responds to the request.

3. TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

3.1 **Standard Contractual Clauses ("SCCs").** Partner agrees that with respect to Personal Data subject to data transfer restrictions under Data Protection Laws and Regulations it shall abide by the relevant terms of the SCCs attached as Schedule 2 to this Processor Addendum. The SCCs shall apply to Partner in its role as Processor as if it were the "data importer." The SCCs shall apply to Tableau and, to the extent legally required, all of Tableau's Affiliates established within the European Economic Area, Switzerland and/or the United Kingdom, in their role as Controllers and these entities shall be deemed "data exporters." Tableau signs the SCCs in name and on behalf of these data exporters. In particular, Partner agrees that as provided in the SCCs, Data Subjects shall be third party beneficiaries to the SCCs.

3.2 **Successor Mechanisms for SCCs.** In the event that (i) the SCCs are amended, replaced or repealed by the European Commission or otherwise under Data Protection Laws and Regulations, or (ii) any DP Regulator (or other supervisory or regulatory authority) requires transfers of Personal Data pursuant to such SCCs to be suspended, the parties shall work together in good faith to enter into any updated version of the SCCs or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws and Regulations. Tableau may terminate this Processor Addendum and the Agreement on 30 days' written notice if the parties are incapable of implementing or fail to implement an appropriate solution to ensure an adequate level of data protection in accordance with Data Protection Laws and Regulations within a period of 90 days.

4. SECURITY INCIDENT RESPONSE

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

5. DATA STORAGE AND DELETION

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

(a) Partner will not store or retain any Protected Information or Confidential Information except as necessary to conduct Partner Activities under the Agreement.

(b) Partner will (i) inform Tableau in writing of all countries where Protected Information is Processed or stored and (ii) obtain consent from Tableau for Processing or storage in the identified countries. As of the Effective Date, Partner may store Protected Information in the countries within the Territory listed in the Agreement, to which Tableau hereby consents. If Partner Processes Personal Data of Tableau's customers, Tableau may make this country list available to Tableau's customers.

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

(a) Within 30 calendar days of the Agreement's expiration or termination, or sooner if requested by Tableau, Partner will securely destroy (per subsection (c) below) all copies of Protected Information and Confidential Information (including any automatically created archival copies).

(b) Upon Tableau's request, Partner will promptly return to Tableau a copy of all Protected Information and Confidential Information within 30 days and, if Tableau also requests deletion of the Protected Information and Confidential Information, will carry that out as set forth above.

(c) All deletion of Protected Information and Confidential Information must be conducted in accordance with best practices for deletion of sensitive data. For example, secure

deletion from a hard drive is defined at a minimum as a seven-pass write over the entire drive.

(d) Tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method, such as shredding performed by a bonded provider.

(e) Upon Tableau's request, Partner will provide a "Certificate of Deletion" certifying that Partner has deleted all Protected Information and Confidential Information. Partner will provide the "Certificate of Deletion" within 30 days of Tableau's request.

6. SUB-PROCESSING

6.1 **Consent for Sub-processing.** Partner will not sub-process, subcontract or delegate any of its obligations under this Processor Addendum without prior written consent of Tableau. Upon receiving consent for current Sub-processors, Partner may add additional Sub-processors provided that it gives 60 days' prior written notification of the identity of the new Sub-processor to Tableau and Tableau does not object to the appointment within that period. In the event Tableau objects to a new Sub-processor, Partner will use reasonable efforts to make available to Tableau a change in the affected Partner Activities to avoid Processing of Protected Information by the objected-to new Sub-processor without unreasonably burdening Tableau. If Partner is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Tableau may terminate this Processor Addendum and the Agreement, and the Partner shall cease Processing Protected Information. For the avoidance of doubt, sub-processing includes any Processing of Protected Information, including access, transmission, or storage by Partner, its Affiliates, or its Sub-processors. Unless Tableau expresses in the consent an intent to allow Partner to sub-process generally, any consent provided by Tableau per this section is limited to the specific Sub-processor for which the consent was provided. Partner's use of Sub-processors shall be subject to the following:

(a) Partner shall be fully responsible for the performance of any Sub-processor and the compliance with all of the obligations of this Processor Addendum by any Sub-processor. To this end, Partner will conduct proper due diligence on all Sub-processors to ensure each Sub-processor can comply with Data Protection Laws and Regulations, all applicable terms and conditions of the Agreement, and all applicable Tableau policies and procedures to which Partner may be subject during the term of the Agreement.

(b) Sub-processors retained by Partner to conduct Partner Activities will at all times be deemed Sub-processors of Partner and shall not under any circumstance be construed or deemed to be employees or Sub-processors of Tableau.

(c) Partner shall ensure that it has a written contract in place with the relevant Sub-processor which meets the same obligations in respect of Processing of Tableau's Protected Information as are imposed on Partner under this Processor Addendum.

(d) Partner shall flow down all obligations in this Processor Addendum regarding, among other things: (i) Protected Information and (ii) all Tableau's and Tableau's DP Regulator's (and, if Partner processes Personal Information of Tableau customers, Tableau's customers and Tableau's customers' DP Regulator's) rights regarding review and audit (including Tableau's right to appoint an independent third party to perform such review or audits).

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

7. **AUDITS**

7.1 **Right to Audit; Permitted Audits.** In addition to any other audit rights described in the Agreement, Tableau and its DP Regulators shall have the right to an on-site audit of Partner's architecture, systems, policies and procedures relevant to the security and integrity of Protected Information, or as otherwise required by a DP Regulator and/or governmental regulator:

(a) Following any notice from Partner to Tableau of an actual or reasonably suspected Security Breach or unauthorized disclosure of Protected Information.

(b) Upon Tableau's reasonable belief that Partner is not in compliance with its security policies and procedures under this Processor Addendum regarding Protected Information.

(c) As required by DP Regulators and/or governmental regulators.

(d) For any reason, or no reason at all, once annually.

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

(a) Conducted by Tableau or its DP Regulator (or, if Partner processes Personal Data of Tableau customers, Tableau's customers and Tableau's customers' DP Regulator's), or through a third party independent contractor selected by one of these parties.

(b) Conducted during reasonable times.

(c) To the extent possible, conducted upon reasonable advance notice to Partner.

(d) Of reasonable duration and shall not unreasonably interfere with Partner's day-to-day operations.

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

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

8. **MISCELLANEOUS TERMS**

8.1 **Legal Process.** If Partner or anyone to whom Partner provides access to Protected Information becomes legally compelled by a court, DP Regulator or other government authority to disclose Protected Information, then to the extent permitted by law, Partner will promptly provide Tableau with sufficient notice of all available details of the legal requirement

and reasonably cooperate with Tableau's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as Tableau may deem appropriate.

8.2 **Conflict.** In the event of any conflict or inconsistency between this Processor Addendum and the Agreement, this Processor Addendum shall prevail.

8.3 **Disclosure of this Addendum.** As required or upon request, Tableau may provide a summary or copy of this Processor Addendum to any DP Regulator and/or government regulator or Tableau customer.

8.4 **Survival.** Partner's obligations under this Processor Addendum will survive expiration or termination of the Agreement and completion of the Partner Activities as long as Partner continues to have access to Protected Information.

8.5 **Suspension.** Tableau may immediately suspend Partner's Processing of Protected Information if Partner is not complying with this Processor Addendum.

8.6 **Termination.** Tableau may terminate the Processor Addendum if Tableau reasonably determines that (a) Partner has failed to cure material noncompliance with the Processor Addendum within a reasonable time; or (b) Tableau needs to do so to comply with Data Protection Laws and Regulations.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses processors

PART A – SCHEDULE 1 - DETAILS OF THE PROCESSING

Categories of Data Subjects

Tableau may provide Personal Data to Partner, the extent of which is determined and controlled by Tableau 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 Tableau (who are natural persons)
- Employees or contact persons of Tableau's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Tableau (who are natural persons)

Categories and nature of Personal Data

Tableau may provide Personal Data to Partner, the extent of which is determined and controlled by Tableau 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

Scope and purpose of Processing

The objective of Processing of Personal Data by Partner is to conduct the Partner Activities as outlined in the Agreement.

Duration of Processing

Subject to the Data Storage and Deletion section of the Processor Addendum, Partner will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

PART A – SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: Tableau Software, LLC

Address: 1621 N. 34th St., Seattle, Washington, 98103, USA

Tel.: + 1 206 634 3400; ; e-mail: privacy@salesforce.com

Other information needed to identify the organisation: Not applicable

(the data **exporter**)

And

Name of the data importing organisation: Partner (and contact information thereof) as identified in the Agreement

Address:

Tel.: e-mail:

Other information needed to identify the organisation: Not applicable

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

Clause 6

Liability

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3

or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter (as such term is applied *mutatis mutandis* per the Partner Processor Addendum) is (please specify briefly your activities relevant to the transfer): Tableau Software, a provider of enterprise cloud and installed computing and data analysis and visualization solutions, signing in name and on behalf of its Affiliates that are based in the European Economic Area and are a Controller.

Data importer

The data importer (as such term is applied *mutatis mutandis* per the Partner Processor Addendum) is (please specify briefly activities relevant to the transfer):

Partner, an authorized Partner of Tableau, performing Partner Activities as authorized and described more fully in the Agreement between Partner and Tableau.

Data subjects

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

Data exporter provide personal data to the data importer, which may include, but is not limited to personal data relating to the following categories of data subjects:

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

Categories of data

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

Data exporter may provide personal data to the data importer 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

Special categories of data (if appropriate)

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

No special categories of data shall be transferred.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of processing of personal data by data importer is the performance of Partner Activities as outlined in the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses:

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data contained in Customer Data, as described in the Processor Addendum. Data Importer will not materially decrease the overall security of the Partner Activities during the term of the Agreement.