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 Module 2: Transfer controller to processor

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

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II– OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it

has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least sixty (60) days prior to the engagement of the sub- processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer 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. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another

EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. 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: Tableau Software, LLC, 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.

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

Contact person's name, position and contact details: Attn: Tableau Legal, + 1 206 634 3400, privacy@salesforce.com.

Activities relevant to the data transferred under these Clauses: The activities as authorized and described in the Agreement.

Signature and date: As accepted via the online process established by Tableau.

Role (controller/processor): Controller

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

Name: Partner name as identified in the Agreement.

Address: The address as laid out in the Agreement.

Contact person's name, position and contact details: The contact information as laid out in the Agreement.

Activities relevant to the data transferred under these Clauses: Partner, an authorized Partner of Tableau, performing Partner Activities as authorized and described in the Agreement.

Signature and date: As accepted via the online process established by Tableau.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- 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 of personal data transferred

- First and last name

- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data

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.

The personal data transferred shall not include sensitive data or special categories of data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous transfer

Nature of the processing

To conduct the Partner Activities as outlined in the Agreement.

Purpose(s) of the data transfer and further processing

Performance of the Partner Activities and fulfilment of data importer's obligations in accordance with the Agreement.

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

Subject to the Data Storage and Deletion section of the Processor Addendum, which forms part of the Agreement between Tableau and Partner, Partner will retain Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing by the parties or unless otherwise required by applicable law.

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

The subject matter and nature of the processing are to perform the services as set forth in the written services agreement with the (sub-) processor, with the duration of the performance of the services as set forth in the written services agreement with the (sub-) processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State, the Data Protection Commission (DPC) in Ireland shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint

a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the Data Protection Commission (DPC) in Ireland shall act as competent supervisory authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data, as described in the Processor Addendum, which forms part of the Agreement between Tableau and Partner (data importer). Data importer will not materially decrease the overall security of the Partner Activities during the term of the Agreement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Where data importer transfers personal data to (sub-) processors, data importer implements and maintains measures for vetting and oversight of its (sub-) processors to protect personal data consistent with these Clauses, including with respect to security obligations and assistance to the controller and/or data exporter as applicable.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: N/A