Traction On Demand Data processing addendum

TRACTION ENTERPRISE CO.

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "DPA") is effective on the effective date of the Agreement.

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data is Processed by ToD under the Agreement.

1. Definitions
1.1 For the purposes of this DPA, the following terms shall have their respective meanings set forth below and other capitalized terms used but not defined in this DPA have the same meanings as set forth in the Agreement:

(a) **“Adequate Country”** means a country or territory that is recognized under EU Data Protection Laws as providing adequate protection for Personal Data.

(b) **“Affiliate”** means, with respect to any party to the DPA, any person, partnership, joint venture, corporation or other entity which directly or indirectly controls, is controlled by, or is under common control with such party where “control” (or variants of it) means the ability to direct the affairs of another by means of ownership, contract or otherwise.

(c) **“Agreement”** means the legal agreement entered into between ToD and Client, to which this DPA is attached or incorporated by reference providing for the provision by ToD to Client of the Services described therein.

(d) **"Controller"** means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data pursuant to Data Protection Laws.

(e) **“Data Protection Laws”** means any and all laws and regulations applicable to the Processing of Personal Data under the Agreement, including EU Data Protection Laws and any other such laws and regulations that take effect during the term of the Agreement.

(f) **“Data Subject”** is a natural person about whom the Controller holds Personal Data and who can be identified, directly or indirectly, by reference to that Personal Data.

(g) **“EEA”** means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

(h) **“EU Data Protection Laws”** means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the

Processing of Personal Data under the Agreement including the General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data) as amended, replaced, or superseded from time to time ("GDPR").

(i) **"Personal Data"** means any information relating to an identified or identifiable natural person. For the purposes of the Agreement and this DPA, Personal Data refers to that of the Client and the Client's customers provided to ToD by Client as necessary for ToD to perform the Services or meet its obligations under the Agreement.

(j) **"Processing"** 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) **"Processor"** means an entity which Processes Personal Data on behalf of the Controller.

(l) **"Security Incident"** means confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data caused by the acts or omissions of ToD, its Affiliates, or Sub-processors.

(m) **"Sensitive Data"** means Personal Data about a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a Data Subject's sex life or sexual orientation, and, without limiting the foregoing, any additional information that falls within the definition of "special categories of data" under Data Protection Laws.

(n) **"Standard Contractual Clauses"** means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as at the Effective Date or any subsequent version thereof released by the European Commission (which will automatically apply).

(o) **"Client"** means the party who entered into the Agreement with ToD and any successor of same.

2. Relationship between DPA and the Agreement

2.1 If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail to the extent the subject matter concerns the Processing of Personal Data.

2.2 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.3 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the jurisdiction set forth in the Agreement for governing law purposes.

3. Permitted Processing, Prohibited Data
3.1 Client consents to ToD Processing Personal Data as permitted by and pursuant to the Agreement, this DPA. The types of Personal Data, the subject matter, duration, nature and purpose of the Processing, and the categories of Data Subjects are detailed at Annex A to this DPA.

3.2 ToD shall Process the Personal Data only in accordance with Client's lawful, written instructions, including as stated herein, except where otherwise required by applicable law. The Agreement and this DPA sets out Client's complete instructions to ToD in relation to the Processing of Personal Data and any Processing required outside of the scope of these instructions will require prior written agreement between the parties. Client acknowledges that ToD shall have a right to Process Personal Data in order to provide the Services to Client, fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Services such as billing, account management, technical maintenance and support, product development, and sales and marketing. Under no circumstances will ToD rent or sell Personal Data.

3.3 Unless the Processing of Sensitive Data is otherwise permitted by Data Protection Laws and Client obtains ToD's prior written consent, Client will not provide (or cause to be provided) any Sensitive Data to ToD for Processing, and ToD will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, the obligations of ToD under this DPA will not apply to Sensitive Data unless the Processing of Sensitive Data is otherwise permitted by Data Protection Laws and Client has obtained ToD's prior written consent.

3.4 Client shall not provide ToD with credit, debit or other payment cardholder information.

4. Client Obligations
4.1 Client shall be responsible for ensuring that:

(a) Client has complied, and will continue to comply, with Data Protection Laws, in Client's use of the Services and Client's own Processing of Personal Data, including by providing notice and obtaining all consents and rights necessary under Data Protection Laws for ToD to process Personal Data;

(b) Client has, and will continue to have, the right to transfer, or provide access to, the Personal Data to ToD for Processing in accordance with the terms of the Agreement and this DPA; and

(c) Client securely uses the Services, including securing Client's account authentication credentials, protecting the security of Personal Data when in transit, and taking any appropriate steps to back up Personal Data.

5. Vendor Obligations

5.1 Security Controls. ToD shall implement and maintain appropriate physical, technical and administrative measures designed to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

5.2 Security Exhibit. The specific physical, technical and administrative security measures which ToD shall have in place are set out at Annex B to this DPA.

5.3 Confidentiality of Processing. ToD shall take reasonable steps to ensure that any person that it authorizes to Process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

5.4 Client Instructions. As soon as reasonably practicable upon becoming aware, inform the Client if, in ToD's opinion, any instructions provided by Client under the Agreement or this DPA violate the GDPR.

5.5 Security Incidents. Upon becoming aware of a Security Incident, ToD shall provide Client with commercially reasonable cooperation and assistance in respect of a Security Incident. Such cooperation and assistance shall include ToD notifying Client of the Security Incident without undue delay and providing the following information in ToD's possession concerning such Security Incident, to the extent known:

(a) the likely causes and consequences for the Data Subjects of the Security Incident;

(b) the categories of Personal Data involved;

(c) a summary of the unauthorized recipients of the Personal Data; and

(d) measures taken by ToD to mitigate any damage.

5.6 ToD shall also provide such timely and reasonable information required by Client to fulfil any data breach reporting obligations required by Data Protection Laws. ToD shall not make any public announcement or notify any Data Subjects without the prior written consent of Client, unless required by applicable law.

5.7 ToD shall take appropriate and commercially reasonable steps to investigate and mitigate the effects of such a Security Incident on the Personal Data under this Agreement.

5.8 This Section does not apply to Security Incidents that are caused by Client, including Client's employees, partners, subcontractors, or agents.

6. International Transfers

6.1 To the extent that the Processing of Personal Data by ToD involves the export of Personal Data to a third party in a country or territory outside the European Union, the European Economic Area, their member states, and the United Kingdom, such export shall be:

(a) to an Adequate Country;

(b) to a third party that is a member of a compliance scheme recognized as offering adequate protection for the rights and freedoms of Data Subjects as determined by the European Commission; or

(c) governed by the Standard Contractual Clauses subject to the additional terms in Annex C, with Client as exporter and ToD as importer.

7. Sub-processors and Affiliates
7.1 Sub-processors. Client agrees that this DPA constitutes Client's written authorization for ToD to engage Affiliates and the third party sub-processors (collectively, "Sub-processors") to Process the Personal Data on ToD's behalf as part of the Services, as detailed here: https://tractionondemand.com/sub-processors/. ToD will notify Client by posting an updated list of Sub-processors at this website, via email, or otherwise as identified by ToD to Client in writing, of any additional Sub-processor being appointed to Process the Personal Data after the effective date of this DPA.

7.2 Objection to Sub-processors. Client may object in writing to the appointment of any additional Sub-processor by stating Client's reasonable grounds for the objection within five (5) calendar days after receipt of ToD's notice in accordance with the mechanism set out at Section 7.1 above. In the event that Client objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, ToD will, at its sole discretion, either not appoint such Sub-Processor, or permit Client to suspend or terminate the Services in accordance with the termination provisions of the Agreement. In the event that Client suspends or terminates the Services in accordance with the preceding sentence, Client shall immediately pay all fees and costs then owing and all fees and costs incurred by ToD as a result of the termination.

7.3 Sub-processor obligations. Where a Sub-processor is engaged by ToD as described in this Section 7, ToD shall:

(a) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and

(b) remain responsible for any breach of this DPA caused by any Sub-processor.

8. Cooperation
8.1 Cooperation and Data Subjects' rights. ToD shall, taking into account the nature of the Processing, provide commercially reasonable assistance to the Client to enable Client to respond to requests from Data Subjects seeking to exercise their rights under Data Protection Laws in the event Client does not have the ability to implement such requests without ToD's assistance. In the event that such requests are made directly to ToD, ToD shall, unless prohibited by applicable law, promptly inform Client of the same. Unless required by applicable law, ToD shall not respond to a Data Subject request without Client's prior written consent except to confirm that such request

relates to Client, to which Client hereby agrees to. Client shall be responsible for any costs arising from ToD's provision of assistance under this Section 8.

8.2 Data Protection Impact Assessments. ToD shall, to the extent required by Data Protection Laws and at Client's sole expense, taking into account the nature of the Processing and the information available to ToD, provide Client with commercially reasonable assistance with data protection impact assessments or consultations with data protection authorities that Client is required to carry out under Data Protection Laws.

9. Security reports and audits
9.1 The parties acknowledge that ToD uses external auditors to comprehensively assess the adequacy of its Personal Data Processing, including the security of the controls used by ToD to provide its Services.

9.2 The parties further acknowledge that these audits:

(a) are performed at least once annually;

(b) are conducted by auditors selected by ToD, but otherwise conducted with all due and necessary independence and professionalism; and

(c) are fully documented in an audit report that assesses whether ToD's controls are consistent with industry standards ("Audit Report").

9.3 At Client's written request and at Client's sole expense, ToD will (on a confidential basis) provide Client with a summary of the Audit Report so that the Client can verify ToD's compliance with the audit standards against which it has been assessed, and this DPA.

9.4 ToD will further provide written responses (on a confidential basis) to reasonable requests for information made by Client in writing, no more than once per year, including responses to information security and audit questionnaires of the Client that are necessary to confirm ToD's compliance with this DPA.

9.5 While it is the parties' intention to rely on the provision of the Audit Report and written responses provided under Sections 9.3 and 9.4 above to verify ToD's compliance with this DPA, ToD shall permit Client (or Client's appointed third party auditors, which must be reasonably acceptable to ToD), at Client's sole expense, to carry out an audit of ToD's Processing of Personal Data under the Agreement following a Security Incident, or upon the instruction of a data protection authority with jurisdiction over the parties and the Processing of Personal Data, to determine ToD's compliance with this DPA. Client must give ToD reasonable prior notice of such intention to audit, conduct the audit during normal business hours, and take all reasonable measures to prevent unnecessary disruption to ToD's operations. Any such audit shall be subject to ToD's security and confidentiality terms and guidelines. Following completion of the audit, upon request, Client will promptly provide ToD with a complete copy of the results of that audit. Notwithstanding the foregoing, ToD will not be required to disclose any proprietary or privileged information, including to Client or any of Client's auditors, agents, or vendors.

10. Deletion / return of data

10.1 Deletion or return of data: Upon the termination or expiration of the Agreement, upon Client's written request, provided such request is made within 30 days of the date of termination or expiration of the Agreement, ToD will make available a CSV extract of Personal Data that is in ToD's possession. At the end of such 30 day period, ToD shall delete or destroy all copies of Personal Data in its possession, save to the extent that: (i) ToD is required by any applicable law to retain some or all of the Personal Data, (ii) ToD is reasonably required to retain some or all of the Personal Data for limited operational and compliance purposes; or (iii) Personal Data has been archived on back-up systems. In all such cases, ToD shall maintain the Personal Data securely and limit processing to the purposes that prevent deletion or return of the Personal Data.

ANNEX A
DESCRIPTION OF PROCESSING

Nature and purposes of Processing
ToD is a Canadian provider of Salesforce.com implementation and application development services. The data Processing will involve any such Processing that is necessary for the purposes set out in the Agreement, the DPA, or as otherwise agreed between the parties in writing.

Categories of Data Subjects
Any categories of individuals whose data Client transfers and/or loads into Client's Salesforce.com instance and data which Client gives ToD access to pursuant to the Agreement and DPA.

Categories of data
The Personal Data concerns the following categories of data for the Data Subjects:

Any Personal Data that Client chooses to include in Client's instance of the Services or that Client gives ToD access to pursuant to the Agreement and DPA.
The Personal Data transferred to ToD for Processing is determined and controlled by Client in Client's sole discretion.

Special categories of data (if appropriate)
ToD does not intentionally collect or Process any Sensitive Data in the provision of the Services.

Client agrees not to provide Sensitive Data to ToD at any time unless Client has met its obligations under and does so pursuant to the Agreement and DPA, including at Sections 3 and 4 of the DPA.

Duration of Processing
The Personal Data will be Processed for the term of the Agreement, or as otherwise required by applicable law or agreed between the parties in writing.

ANNEX B
TRACTION SECURITY MEASURES

1. Network-Level Controls
a. ToD will use host-based firewall(s) to protect hosts/infrastructure handling Personal Data. The firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.

b. ToD will have network-based security monitoring for the segment(s) on which hosts handling Personal Data are logically located.

c. ToD will assess network-level vulnerabilities and address critical vulnerabilities within a reasonable period of time.

d. ToD will employ change management standards for network/infrastructure components handling Personal Data.

2. Server-Level Controls
a. ToD will implement operating system hardening for hosts/infrastructure handling Personal Data. Operating system hardening includes, but is not limited to, the following configurations: strong password authentication/use of keys, inactivity time-out, disabling or removal of unused or expired accounts and services, turning off unused ports, and log management. In addition, ToD will implement access control Processes and restrict access to operating system configurations based on the least privilege principle.

b. ToD will perform patch management on systems that host or handle Personal Data. ToD will implement critical patches within vendor recommended timeframes on systems that host or handle Personal Data within a reasonable period of time.

c. ToD will implement specific controls to log activities of users with elevated access to systems that host or handle Personal Data.

d. ToD will, at a minimum, assess system-level vulnerabilities on a monthly basis and address critical vulnerabilities within a reasonable period of time.

e. ToD will employ a comprehensive antivirus or endpoint security solution for endpoints which handle Personal Data.

f. Physical servers will be protected with appropriate physical security mechanisms, including but not limited to key card access, cameras, alarms, and enforced user provisioning controls.

3. Application-Level Controls
a. ToD will maintain documentation on overall application architecture, Process flows, and security features for applications handling Personal Data.

b. ToD will employ secure programming guidelines and protocols in the development of applications Processing or handling Personal Data.

c. ToD will regularly perform patch management on applications that host or handle Personal Data. ToD will implement critical patches within vendor recommended timeframes on all applications that host or handle Personal Data, within a reasonable period of time.

d. ToD will, at a minimum, assess application-level vulnerabilities on a monthly basis and address critical vulnerabilities within a reasonable period of time.

e. ToD will perform code review and maintain documentation of code reviews performed for applications that host or handle Personal Data.

f. ToD will employ change management standards for applications hosting or handling Personal Data.

4. Data-Level Controls
a. ToD will use strong encryption (TLS) for transmission of Personal Data that is considered Confidential Information. Data backups of Personal Data will be encrypted at rest and while in transit. All of ToD's databases are also encrypted at rest.

5. End User Computing Level Controls
a. ToD will employ an end point security or antivirus solution for end user computing devices that handle Personal Data.

b. ToD will ensure that end user computing devices that handle Personal Data are encrypted.

c. ToD will ensure that end user access is controlled by, including but not limited to, the following configurations: strong password authentication/multi factor authentication.

d. ToD will implement critical patches on systems that host or handle Personal Data within a reasonable period of time after the patch is identified.

6. Compliance Controls
a. ToD will make a good faith effort to operate within the parameters of ToD's then-current Information Security Policy.

b. Notwithstanding any of the foregoing, ToD will adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to, building access control, employee education and personnel security measures.

ANNEX C
STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

Client is the data exporter and ToD is the data importer and the parties agree to the following. If and to the extent an authorized Affiliate relies on the EU C-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Client' in this Schedule, include such authorized Affiliate.

a. Reference to the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this ADDENDUM. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Annex C(o).

b. Docking clause. The option under clause 7 shall not apply.

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

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

e. Security of Processing. For the purposes of clause 8.6(a), Client is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in the security, privacy and architecture documentation meet Client's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by ToD provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 5 of this ADDENDUM.

f. Audits of the SCCs. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 9 of this ADDENDUM.

g. General authorisation for use of Sub-processors. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), ToD has Client's general authorisation to engage Sub-processors in

accordance with section 7 of this ADDENDUM. ToD shall make available to Client the current list of Sub-processors in accordance with section 7 of this ADDENDUM. Where ToD enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Client hereby grants ToD and ToD's Affiliates authority to provide a general authorisation on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

h. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to clause 9(a), Client acknowledges and expressly agrees that ToD may engage new Sub-processors in accordance with section 7 of this ADDENDUM. ToD shall inform Client of any changes to Sub-processors following the procedure provided for in section 7of this ADDENDUM.

i. **Complaints - Redress**. For the purposes of clause 11, and subject to section 8 of this ADDENDUM, ToD shall inform data subjects on its website of a contact point authorised to handle complaints. ToD shall inform Client if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Client. ToD shall not otherwise have any obligation to handle the request (unless otherwise agreed with Client). The option under clause 11 shall not apply.

j. **Liability**. ToD's liability under clause 12(b) shall be limited to any damage caused by its Processing where ToD has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Client, as specified in Article 82 GDPR.

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

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

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

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

having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as competent supervisory authority.

iv. Where Client is established in the United Kingdom or falls within the territorial scope of application of UK Applicable Law, the Information Commissioner's Office shall act as competent supervisory authority.

v. Where Client is established in Switzerland or falls within the territorial scope of application of Swiss Applicable Law, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Applicable Law.

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

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

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

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

i. The contents of ANNEX A, B, and C shall form Annex I.A to the Standard Contractual Clauses
ii. The contents of Annex A shall form Annex I.B to the Standard Contractual Clauses
iii. The contents of Annex C (k) shall form Annex I.C to the Standard Contractual Clauses
iv. The contents of Annex B shall form Annex II to the Standard Contractual Clauses.

p. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses**.

In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Applicable Law of Switzerland ("Swiss Applicable Law"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Applicable Law of the United Kingdom ("UK Applicable Law") or Swiss Applicable Law, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Applicable Law or Swiss Applicable Law, as applicable. In respect of data transfers governed by Swiss Applicable Law, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Applicable Law until such laws are amended to no longer apply to a legal entity.

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

Last Updated April 8, 2022.