DATA PRIVACY ADDENDUM ("DPA")

1. In addition to the Agreement, this DPA applies whenever Service Provider Processes any Personal Data protected by the Privacy Regulations from or on behalf of on behalf of McKinsey, any McKinsey Affiliate, any McKinsey client, or otherwise under the Agreement and/or any SOW.

2. Definitions. All other defined terms used and not otherwise defined herein shall have the meanings defined in the Agreement between the Parties.

   a. "**Data Subjects**" has the meaning set out below.

   b. "**Personal Data**" means any information, whether accurate or not, and whether recorded in a material form or not, that relates to an identified or identifiable natural person ("**Data Subject**") that can be identified, directly or indirectly, by reference to an identifier or one or more characteristics, or is otherwise "personal data," "personal information," "personally identifiable information," or any other information regulated by applicable Privacy Regulations, that Service Provider processes in the interest or on behalf of McKinsey.

   c. "**Privacy Regulations**" has the meaning set out in the Agreement.

   d. "**Process**" and "**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, combination, restriction, erasure or destruction, and any other activity with respect to Personal Data that is governed by applicable Privacy Regulations.

   e. "**Sub-Processor**" means any third party that Service Provider uses to Process Personal Data, and any downstream third party that Processes Personal Data on behalf of such subcontractor.

3. Amendments. The Parties shall negotiate in good faith in order to revise the terms and conditions of this DPA when necessary to reflect any changes in applicable Privacy Regulations.

4. Transfers. Service Provider shall not transfer McKinsey's, McKinsey Affiliate's or McKinsey client's Personal Data to a third country without McKinsey's prior written consent. Insofar as the Services involve the transfer of Personal Data and any Privacy Regulations require that additional steps or safeguards be imposed before the data can be transferred to a second jurisdiction, the Parties agree to the following terms, which are incorporated herein by reference: https://solutions.mckinsey.com/msd/service-providers/docs/Standard-Contractual-Clauses.pdf and shall cooperate to enter into such other standard agreements as may be required by Privacy Regulations (collectively, "Standard Contractual Clauses or "SCCs").

5. Processing. In respect of the Personal Data that Service Provider is Processing (whether directly or indirectly) in connection with, or in performance of, the Agreement and/or applicable SOW, Service Provider shall, and shall procure that its employees, Sub-Processors, and agents shall comply with this Section 5 of this DPA.

   a. Subject to Service Provider's compliance with this DPA, McKinsey agrees to make Personal Data available to Service Provider for the business purpose of providing the Services as contemplated by the Agreement and/or applicable SOW (the "Specified Business Purpose"). McKinsey reserves the right to take reasonable and appropriate steps to help ensure that Service Provider Processes Personal Data in a manner consistent with McKinsey's obligations under applicable Privacy Regulations, including without limitation the right, upon notice, to stop and remediate any unauthorized Processing of Personal Data.

   b. Service Provider acknowledges that Personal Data Processed by Service Provider may be Personal Data of which McKinsey or its clients is/are the data controller under the Privacy Regulations. Service Provider shall Process Personal Data only on behalf of and for the benefit of McKinsey and/or its clients, and solely to carry out its obligations pursuant to the Agreement and/or applicable SOW or McKinsey's written instructions, unless otherwise required by any applicable law (in which event, Service Provider shall inform McKinsey of the legal requirement before Processing Personal Data other than in accordance with McKinsey's instructions, unless that same law prohibits Service Provider from informing McKinsey). Service Provider certifies that it (a) understands the obligations and restrictions imposed on it by applicable Privacy Regulations in its role as a processor; (b) shall comply with all such obligations; and (c) shall notify McKinsey immediately if Service Provider determines that it can no longer meet its obligations under applicable Privacy Regulations or this Section. Service Provider shall immediately notify McKinsey if, in its opinion, a Processing instruction infringes applicable Privacy Regulations.

Personal Data is McKinsey's Confidential Information; *provided*, however, the Confidential Information Exceptions do not apply to Personal Data.

c. Unless otherwise agreed by the Parties in writing, the subject-matter, duration, nature and purpose, types of Personal Data, categories of Data Subject Processed, and any other relevant details required under the Privacy Regulations are specified in the applicable SOW and/or the SCCs.

d. Service Provider shall not: (i) transfer, communicate, disclose or otherwise make Personal Data available to third parties in exchange for monetary or other valuable consideration (includes "selling" as defined in CCPA and similar terms under other Privacy Regulations); (ii) transfer, communicate, disclose, or otherwise make Personal Data available to third parties for their use in delivering interest-based advertising (also referred to as "targeted advertising" or "cross-context behavioral advertising"; includes "sharing" as defined in the California Consumer Privacy Act, as amended ("**CCPA**") and similar terms under other Privacy Regulations); (iii) retain, use or disclose Personal Data for any purpose, other than for the Specified Business Purpose; (iv) retain, use, or disclose Personal Data outside the direct business relationship between the Parties hereunder; (v) attempt to identify or reidentify individuals using deidentified data that it receives from McKinsey or permit any entity acting on Service Provider's behalf to do so; or (vi) combine Personal Data with personal data that Service Provider received from or on behalf of another person or entity or collects from its own interactions with an individual. Service Provider certifies that it understands the restrictions contained in this paragraph and will comply with them.

e. Service Provider shall provide at least the same level of privacy and security protection for Personal Data as is required by applicable Privacy Regulations (including the Privacy Regulations in the country where the Data Subjects of the Personal Data are located). Service Provider represents and warrants that it has implemented technical, organizational, personnel and physical measures appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation, including the requirements in this Section.

f. Service Provider shall not engage any Sub-Processor without notifying McKinsey and obtaining McKinsey's prior written authorization. Notwithstanding the foregoing, McKinsey hereby authorizes those Sub-Processors disclosed to McKinsey as of the Effective Date, provided that any subsequent change to the list of pre-approved Sub-Processors must be authorized by McKinsey. Notwithstanding the above, Service Provider shall not transfer, disclose or allow access to the Personal Data to any Sub-Processor, except to the extent required for the performance of its obligations under the Agreement and/or the applicable SOW. Service Provider shall impose binding obligations which are the same or reasonably equivalent to those in this DPA with its Sub-Processors. Service Provider shall ensure that all Sub-Processors comply with Service Provider's obligations hereunder and shall be liable for any act or omission by its Sub-Processors.

g. Service Provider shall: (i) taking into account the nature of the Services, provide reasonable assistance to McKinsey, insofar as this is possible, for the fulfilment of McKinsey's obligations under applicable Privacy Regulations in respect of data security, data breach notification, data protection impact assessments, prior consultation with supervisory authorities and the fulfilment of Data Subjects' rights; (ii) notify McKinsey promptly, but within no more than three (3) days (or within a shorter time period, if this is required under applicable Privacy Regulations) of any enquiry or complaint received from an individual, competent court or regulatory authority in relation to Personal Data; and (iii) make available to McKinsey upon request all information necessary to demonstrate the compliance of Service Provider and any sub-contractors with Privacy Regulations and with Section 7 (Confidentiality) and Section 8 (Security) of the Agreement, and this DPA, and allow for and contribute to audits (including audits of its sub-contractors (either (1) directly by McKinsey or its representatives or (2) indirectly through the Service Provider at the sole discretion of McKinsey), to the extent that such audits are expressly required or permitted under applicable Privacy Regulations) conducted by McKinsey or its representatives bound by appropriate obligations of confidentiality. Service Provider acknowledges and agrees that, to the extent required under applicable Privacy Regulations, Data Subjects are third party beneficiaries to the Agreement and this DPA.

h. Within thirty-six (36) hours after discovery of a Security Incident (as defined in the Agreement) that involves Personal Data, Service Provider shall notify McKinsey of the existence of this Security Incident and provide to McKinsey, as soon as it received the information, all information required under any applicable Privacy Regulations, including but not limited to the nature of the Personal Data subject to the Security Incident, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; the name and contact details of the data protection officer or other contact point where more information can be obtained; the likely consequences of the Security Incident; the measures taken or proposed to be taken by Service Provider to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects and any other information as McKinsey may reasonable request. Service Provider shall take all necessary steps to remediate the Security Incident immediately upon discovery . Service Provider shall coordinate with McKinsey in providing notice and credit monitoring to any individuals whose Personal Data may be compromised by the Security Incident and cover any related expenses. Service Provider shall be responsible for any such Security Incident and for any loss, cost, damage, expense (including attorneys' fees and disbursements), liability, penalty, or claim of any nature whatsoever suffered by McKinsey or any McKinsey Affiliate in connection with such Security Incident.

i. Immediately upon expiration or termination of the Agreement, applicable SOW or this DPA, or upon McKinsey's request, Service Provider shall promptly return to McKinsey (or, at McKinsey's request, securely destroy using industry standard methods), all copies of McKinsey's Personal Data, and shall certify in writing its compliance with this Section upon McKinsey's request. Service Provider's obligations under this DPA shall survive until such time as all Personal Data has been returned or securely destroyed. In addition, Service Provider shall promptly comply with any request from McKinsey to correct, transfer or delete the Personal Data, or to otherwise comply with a Data Subject's privacy right.

j. Service Provider shall not misappropriate, nor make any unauthorized alteration to, all or any part of Personal Data except in accordance with applicable Privacy Regulations and to the extent necessary for providing the Services.

k. Service Provider shall make a reasonable effort to ensure that Personal Data is accurate and complete, if such data is likely to be (i) used by Service Provider to make a decision that affects the individual to whom such Personal Data relates, or (ii) disclosed by Service Provider to another organization (where permitted by McKinsey).

l. Service Provider shall ensure that its employees, agents and Sub-Processors (if applicable): (1) can only access Personal Data on a "need to know" basis for purposes of satisfying Service Provider's obligations under the Agreement, are aware of Service Provider's obligations specified in this DPA and are under binding obligations to abide by the same; and (2) are under an appropriate obligation of confidentiality.

m. When Service Provider is notified of a correction of Personal Data, correct the Personal Data unless McKinsey is satisfied on reasonable grounds that the correction should not be made. If no correction is made, Service Provider shall annotate McKinsey Personal Data in its possession or under its control with the correction that was requested but not made.

n. Service Provider shall undertake such training and implement such procedures as may be reasonably required in respect of the Privacy Regulations.

6. Where Service Provider is collecting Personal Data directly from individuals in connection with the Agreement and/or applicable SOW, including from its employees, Service Provider confirms that it has (a) complied with any necessary notification requirements under the Privacy Regulations, (b) obtained sufficient authorization (including obtaining informed consent if required) under the Privacy Regulations from such individuals to enable the Processing of Personal Data as contemplated under the Agreement and/or applicable SOW, and (c) satisfied any other requirements under the Privacy Regulations in connection with the collection of Personal Data from individuals. For the avoidance of doubt, such Personal Data collected by Service Provider in connection with the Agreement and/or applicable SOW may include Service Provider employees' business contact information that is shared with McKinsey for the purposes of facilitating a normal and customary business relationship (e.g. communication, invoicing etc.).

7. Service Provider acknowledges and agrees that McKinsey (or its agents) may, in connection with the Agreement and/or applicable SOW, collect Personal Data from Service Provider or any personnel connected with Service Provider, Process such Personal Data and disclose it to affiliated or unaffiliated third parties including its employees, agents, Sub-Processors, which may be located in jurisdictions outside the jurisdiction where the relevant Personal Data was collected (including to jurisdictions that provide less protection than the jurisdiction in which the Personal Data was originally collected), for purposes connected with the Agreement and/or applicable SOW, and if permitted by applicable Privacy Regulations, for the purposes of its legitimate interests or as permitted or required by any applicable law.

8. Service Provider acknowledges and agrees that any breach or threatened breach of this DPA by Service Provider may cause McKinsey immediate and irreparable harm for which damages alone may not be an adequate remedy. Service Provider agrees that McKinsey may commence proceedings to restrain any breach or threatened breach of the terms of this DPA.

9. Disputes in relation to Personal Data that is the subject of this DPA will be governed by and constructed in accordance with the applicable jurisdiction's Privacy Regulations applicable to the Personal Data that is the subject of the dispute.