Data Protection Agreement for US Market Research

This Data Protection Agreement for US Market Research ("**US DPA"**), when incorporated by reference therein, supplements, amends and forms part of the Prodege Market Research Master Services Agreement ("**MRMSA**") or other present or future master services agreement, statement of work, insertion order, or written business understanding (collectively, the "**Agreement**") between Prodege, LLC and its affiliates (collectively, "**Prodege**") and the Prodege market research client that is counterparty to that Agreement and its affiliates (collectively, "**Company**") (each a "**Party**," and together, the "**Parties**"). Pursuant to the Agreement, Prodege may provide market research services ("**Services**") involving the Processing of "personal information" or "personal data"—as these terms are defined under Data Protection Laws (collectively "**Personal Information**")—for or on behalf of Company. To the extent this US DPA and the Agreement conflict with respect to any subject matter herein, this US DPA will control, unless expressly agreed otherwise in writing.

A. **Scope.** Unless the Parties agree otherwise in writing, the scope of this US DPA will be as follows:

   i. Data Subjects. This US DPA applies where Prodege's Services involve the Processing of Personal Information of Data Subjects located in the United States.

   ii. Nature of Processing. Prodege will Process Company Data as Company's Service Provider/Processor. Prodege is a Business/Controller of User Data and shall Process such data in accordance with its own privacy policy and applicable Data Protection Laws. To the extent Company Processes any User Data containing Personal Information, it will do so as an independent Business/Controller or Third Party, in each case subject to the restrictions in this US DPA and the Agreement. Notwithstanding the foregoing, the Parties agree that Data Subjects' Intentional Use of Prodege to disclose User Data to Company (or a third party at Company's direction) will position Company as an independent Business/Controller with respect to such data under applicable Data Protection Laws.

B. **Definitions**. This US DPA uses the following definitions. Capitalized terms used but not defined here have the meaning given to them in the MRMSA or Data Protection Laws, as applicable.

   i. **"Business Purposes"** means the enumerated business purposes set forth in Cal. Civ. Code section 1798.140(e)(1)-(8) that are applicable to and compatible with the Services set forth in the Agreement, including but not limited to: performing services on behalf of Company, such as designing, hosting, conducting, or analyzing surveys or their results, maintaining or servicing accounts, providing customer service, processing transactions, verifying information, providing analytic services, providing storage or other similar services on behalf of Company; auditing the amount, positioning and quality of ad (survey) impressions; helping to ensure security and integrity, to the extent

reasonably necessary and proportionate for these purposes; debugging to identify and repair errors that impair existing intended functionality; internal research for technological development and demonstration; and verifying or maintaining the quality or safety of a service made for or controlled by Company.

ii. **"Company Data"** has the meaning provided in the MRMSA.

iii. **"Covered Data Transaction"** means any prohibited or restricted "transaction" with a "country of concern" or "covered person" involving "United States Government-related data" or "bulk" "sensitive personal data" of US data subjects under Executive Order (EO) 14117 of February 28, 2024 [*Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*] and implementing regulations (as amended), for which no valid exemption or license applies.

iv. **"Data Protection Laws"** means U.S. federal and/or state data security, confidentiality, and/or privacy laws, rules, and regulations that are now or may become applicable to Prodege, the Services, Company Data, User Data, and/or any other Personal Information, programs, or products provided pursuant to the Agreement during its term, as and when these laws take effect, and as amended, superseded, or replaced.

v. **"Data Subject"** means the individual to whom Personal Information relates.

vi. **"Data Subject Access Request"** means a request from a Data Subject to exercise one or more enumerated rights under applicable Data Protection Laws.

vii. **"Intentional Use"** means that a Data Subject has intentionally used, authorized or directed a Party to: (i) make available, transfer or disclose that Data Subject's Personal Information, including to the other Party, or (ii) interact with one or more third parties, including for purposes of providing a product or service requested by the Data Subject.

i. **"Security Incident"** means a breach of Prodege's or its Subprocessors' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Data. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Company Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

viii. **"Subprocessor"** means any third-party Processor engaged by Prodege to Process Company Data.

ix. **"User Data"** has the meaning provided in the MRMSA.

C. **Company Data**. To the extent Prodege Processes Company Data as Company's Service Provider/Processor, the following provisions shall apply:

i. Details of Processing. The subject matter, duration, nature, and purpose of Prodege's Processing, and the types of Personal Information and categories of Data Subjects, are as set forth in this US DPA and the Agreement.

ii. Company Responsibilities. Company represents, warrants, and covenants that it will have and maintain all necessary rights, consents, and authority, including providing any

required notices to Data Subjects, for Prodege to Process Company Data in compliance with applicable Data Protection Laws and this US DPA.

iii. Processing Instructions. Prodege may Process Company Data for purposes of performing the Services, to carry out the Businesses Purposes set forth in this US DPA and the Agreement, as otherwise required or permitted for a Service Provider/Processor under applicable Data Protection Laws, or as agreed or instructed by Company including, without limitation, in the Agreement. Without limiting the generality of the foregoing, unless otherwise agreed in writing, Prodege shall not:

a. Sell or Share Company Data;
b. retain, use, or disclose Company Data for any purpose—including any commercial purpose—that is not a Business Purpose set forth in the Agreement, or as otherwise permitted by applicable Data Protection Laws;
c. retain, use, or disclose Company Data outside of the direct business relationship between Company and Prodege; or
d. combine Company Data received from or on behalf of Company with Personal Information that Prodege receives from or on behalf of another person, or collects from its own interaction with a consumer, except where permitted by applicable Data Protection Laws.

iv. Prodege Responsibilities. In Processing Company Data, Prodege shall:

a. comply with applicable Data Protection Laws;
b. upon Company's reasonable request, make available to Company information in Prodege's possession necessary to demonstrate Prodege's compliance with its obligations under Data Protection Laws (subject to time and materials charges at standard rates for efforts that require material effort);
c. ensure the reasonable security of Company Data including by: (i) providing the same level of privacy protection to Company Data as is required by Data Protection Laws and (ii) ensure each person Processing Company Data is subject to a duty of confidentiality with respect to such Company Data;
d. notify Company of Security Incidents affecting Prodege's Processing of Company Data that require notification to Data Subjects and/or government authorities under Data Protection Laws;
e. provide Company with necessary information to reasonably enable Company to conduct and document data protection assessments (subject to time and materials charges at standard rates for efforts that require material effort);
f. upon Company's request, provide reasonable assistance to enable Company to fulfill Data Subject Access Requests (subject to time and materials charges at standard rates for efforts that require material effort);
g. delete Company Data at the end of performing the Services, or as otherwise instructed by Company, unless retention is: (i) required by applicable laws; (ii) required pursuant to backup or record-keeping procedures, provided that retention is only for such purposes and for as long as reasonably necessary; or (iii) in an anonymized or deidentified form, in which case Prodege may retain and continue to Process such data for legitimate business purposes, provided it no longer constitutes Personal Information under applicable Data Protection Laws;

h. not more than once annually, allow and cooperate with reasonable assessments by Company of Prodege's policies and technical and organizational measures in support of Company's obligations under applicable Data Protection Laws, using an appropriate and accepted control standard or framework and assessment procedure for such assessments, subject to reasonable access and confidentiality restrictions, and subject to time and materials charges at standard rates for efforts that require material effort (where permitted by Data Protection Laws);
i. notify Company if Prodege determines it can no longer meet its obligations under Data Protection Laws and allow Company to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Company Data.

v. Subprocessors. Company provides general authorization for Prodege to use Subprocessors to carry out Processing activities involving Company Data in accordance with this section:
   a. Prodege maintains a list (at www.prodege.com/mrterms/subprocessors/) of its current Subprocessors for the Services, which Company acknowledges and agrees may be used hereunder;
   b. Prodege may engage additional Subprocessors to Process Company Data provided it: (i) gives Company an opportunity to object; and (ii) enters into a written agreement with each Subprocessor imposing substantially the same obligations with respect to Company Data as Prodege has under Section (C) of this US DPA.

D. **User Data.** To the extent Prodege provides Company with access to User Data, the following provisions apply:

i. Prodege's Responsibilities. Where Prodege Sells User Data to or Shares User Data with Company, Prodege represents, warrants and covenants that it will have and maintain all necessary rights, consents, and authority, including providing any required notices to Data Subjects, for Company to Process User Data in compliance with applicable Data Protection Laws and Section (D) of this US DPA.

ii. Company Permitted Purposes. Company may Process User Data solely for the limited purpose(s) specified in the Agreement under which the data was made available (including, as applicable, analytical services; respondent verification or matching, including using tracking technologies; follow-up questionnaire or interview; in-home use test; or data append) (collectively, the **"Specified Purpose"**).

iii. Company's Responsibilities. Company represents, warrants, and covenants that in Processing User Data it will:
   a. comply with applicable Data Protection Laws, including providing the same level of privacy protection for User Data as is required of a Controller/Business;
   b. not Sell or Share User Data;
   c. implement and maintain reasonable security procedures and practices to protect User Data from unauthorized or illegal access, destruction, use, modification or disclosure;

d. notify Prodege in the event Company determines it can no longer meet its obligations under applicable Data Protection Laws; and
e. return or permanently destroy all User Data, and certify that it has been returned or destroyed, once no longer needed for the Specified Purpose or upon written notice from Prodege.

iv. Prodege's Rights. Prodege will have the right, with respect to any User Data made available to Company, to take reasonable and appropriate steps to:
a. ensure Company uses User Data in accordance with applicable Data Protection Laws and this US DPA; and
b. stop and remediate any unauthorized use by Company, upon notice.

v. Demonstration of Compliance. If either Party receives any complaint, notice, or communication from a Data Subject or authority which relates to the other Party's Processing of User Data, or potential failure to comply with applicable laws, that Party shall direct the Data Subject or authority to the relevant Party and provide reasonably necessary assistance to the other Party in responding to the Data Subject or authority.

E. **Deidentified Data.** To the extent Company receives or creates deidentified User Data, or Prodege receives or creates deidentified Company Data, in each case that Party shall: (i) maintain such information as deidentified and take reasonable measures to ensure that it cannot be associated with an individual or household (including implementing technical safeguards and business processes to prevent reidentification or inadvertent release of the deidentified data); (ii) publicly commit to maintain and use the information in deidentified form and not attempt to reidentify the information; (iii) not attribute the other Party as a source of such data; and (iv) contractually obligate any third parties receiving such information to commit to (i), (ii), and (iii).

F. **Covered Data Transactions.** Company agrees not to direct, permit, or facilitate any Covered Data Transaction involving User Data or Company Data obtained from Prodege under the Agreement. Company will notify Prodege within 72 hours of any known or suspected breach of this section F and cooperate in making any required disclosures to U.S. authorities.

G. **Effective Date and Termination.**

i. This US DPA is effective as of the earlier of the date that Company either:
a. executes the US DPA;
b. enters into the Agreement incorporating it by reference; or
c. instructs Prodege to begin Processing Company Data relating to US Data Subjects in connection with Services offered subject to the Agreement.

ii. The provisions of this US DPA that are reasonably expected to survive termination (e.g., compliance with Data Protection Laws; restrictions on data usage; data return, security, and destruction obligations) shall survive termination of the Agreement.