Data Protection Agreement
for Market Research Clients

This Data Protection Agreement (**"DPA"**) for Market Research Clients 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 has executed below 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 DPA and the Agreement conflict with respect to any subject matter herein, this DPA will control, unless expressly agreed otherwise in writing.

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

   i. Data Subjects. This DPA applies to Prodege's Processing of Personal Information of Data Subjects located anywhere, including in the United States and Europe.

   ii. Nature of Processing. Prodege will Process Company Data as Company's Processor. Prodege is a 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 either: (i) an independent Controller or (ii) a Third Party (under applicable US State Privacy Laws), in each case subject to the restrictions in this DPA and the Agreement.

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

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

   ii. **"Controller"** means any natural or legal person which, alone or jointly with others, determines the purposes and means of Processing Personal Information, including a "business" as defined under the CCPA.

   iii. **"Data Privacy Framework"** or "**DPF**" means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce, as amended, superseded, or replaced.

   iv. **"DPF Principles"** means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded, or replaced.

v. **"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.

vi. **"Data Protection Laws"** means all data protection, privacy, and/or security 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, including, without limitation, European Data Protection Laws and US State Privacy Laws, as amended, superseded, or replaced.

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

viii. **"Europe"** means the European Economic Area (**"EEA"**) and its Member States, Switzerland, and the United Kingdom (**"UK"**).

ix. **"European Data Protection Laws"** means applicable Data Protection Laws of Europe that govern the Processing of Personal Information, including the GDPR, UK GDPR, and the Swiss FADP, as amended, superseded, or replaced.

x. **"EU Standard Contractual Clauses"** or **"EU SCCs"** means the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, currently available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as amended, superseded, or replaced.

xi. **"GDPR"** means the General Data Protection Regulation (EU) 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, superseded, or replaced.

xii. **"Processor"** means any natural or legal person which Processes Personal Information on behalf of a Controller, including a "service provider" as defined under the CCPA.

xiii. **"Prodege Permitted Purposes"** means the following purposes: (1) to provide the Services in accordance with the Agreement; (ii) to prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity; (iii) to comply with applicable laws and legal processes; (iv) to exercise or defend legal claims; and (v) for other purposes permitted under applicable Data Protection Laws for a Processor.

xiv. **"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.

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

xvi. **"Swiss FADP"** means the Swiss Federal Act on Data Protection 2020 and its Ordinance, as amended, superseded, or replaced.

xvii. **"Third Country"** means any country outside Europe that does not provide an adequate level of protection for Personal Information within the meaning of applicable Data Protection Laws.

xviii. **"US State Privacy Laws"** means applicable Data Protection Laws of the various US states that govern the Processing of Personal Information, including without limitation the California Consumer Privacy Act, Colorado Privacy Act, Connecticut Privacy Act, Indiana Consumer Protection Act, Iowa Consumer Data Protection Act, Kentucky Consumer Data Protection Act, Maryland Online Data Privacy Act, Minnesota Consumer Data Privacy Act, Montana Consumer Data Privacy Act, Nebraska Data Privacy Act, Nevada Privacy of Information Collected on the Internet from Consumers Act, New Hampshire Act Relative to the Expectation of Privacy, New Jersey Act Concerning Online Services, Oregon Consumer Privacy Act, Rhode Island Data Transparency and Privacy Protection Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, Virginia Consumer Data Protection Law, and any implementing regulations thereunder, in each case as and when these laws take effect, and as amended, superseded, or replaced.

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

xx. **"UK Addendum"** means the International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers, currently available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/, as amended, superseded, or replaced.

xxi. **"UK GDPR"** means the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018, as amended, superseded, or replaced.

C. **Company Data**. To the extent Prodege Processes Company Data as Company's 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 set forth in **Appendix 1** to this DPA.

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, the Agreement, and this DPA.

iii. Processing Instructions. Prodege may Process Company Data solely for purposes of performing the Services and to carry out the Prodege Permitted Purposes, as described under the Agreement and this DPA, or as otherwise agreed or instructed by Company in writing. If Prodege receives a Processing instruction from Company that, in its opinion, infringes Data Protection Laws, it shall promptly inform Company.

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. implement and maintain reasonable technical and organizational measures designed to protect Company Data, as set forth in **Appendix 2** to this DPA, which Prodege may update or modify from time to time provided that such changes do not decrease the overall level of security;
d. ensure that each person Processing Company Data is subject to a duty of confidentiality;
e. 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;
f. provide reasonable assistance and information regarding any Security Incident, as may be required for the purposes of reporting to the authorities and, where necessary, to the Data Subjects;
g. upon Company's request, provide reasonable assistance to enable Company to respond to Data Subjects requests under applicable Data Protection Laws, including, without limitation, requests to access, correct, delete, restrict, object to Processing, or opt out from the sale or sharing of Personal Information (subject to time and materials charges at standard rates for efforts that require material effort, where legally permitted);
h. provide Company with the information reasonably necessary for Company to conduct and document data protection impact assessments and consult with authorities, where legally required (and where permitted, subject to time and materials charges at standard rates for efforts that require material effort) under applicable Data Protection Laws;
i. delete or return 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 accordance with applicable Data Protection Laws, 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; and
j. 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).

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 will enter into a written agreement with each Subprocessor imposing substantially the same obligations with respect to Company Data as Prodege has under this DPA;
   c. Prodege will remain liable for any acts or omissions of its Subprocessors that cause Prodege to breach its obligations under this DPA; and
   d. Prodege may engage additional Subprocessors to Process Company Data provided it (i) notifies Company in advance; and (ii) gives Company an opportunity to object to their engagement on reasonable data protection grounds. The Parties shall discuss any objection in good faith to achieve a commercially reasonable resolution. If no such resolution is reached, Prodege may, at its discretion, either not appoint the Subprocessor or permit Company to terminate the affected part of the Services in accordance with the termination provisions under the Agreement, without liability to either Party (but without prejudice to any fees or costs incurred by Company prior to such termination). This termination right shall be Company's sole and exclusive remedy in the event of an unresolved objection to any new or replacement Subprocessor.

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

i. Prodege's Responsibilities. Prodege represents, warrants and covenants that it will have and maintain all necessary rights, consents, and authority for Company to Process User Data in compliance with applicable Data Protection Laws, the Agreement, and this 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 Purposes"**).

iii. Company's Responsibilities. Company represents, warrants, and covenants that it will:
   a. Process User Data only for the Specified Purposes, and in accordance with any restrictions set forth in the Agreement and this DPA;

b. not use User Data for profiling or automated decision-making, as those terms are defined under applicable Data Protection Laws;
c. implement and maintain reasonable security procedures and practices to protect User Data from unauthorized or illegal access, destruction, use, modification or disclosure; and
d. return or permanently destroy all User Data, and certify that it has been returned or destroyed, once no longer needed for the specific purpose(s) for which it was made available under the Agreement.

iv. 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. **Additional Terms for U.S. Data.**

i. Scope of Application. This Section E applies solely to the extent that either Party Processes Personal Information relating to US data subjects ("US Personal Information") that is received from or Processed on behalf of the other Party for purposes of the Agreement.

ii. Company Data. In Processing Company Data that contains Personal Information subject to US State Privacy Laws, Prodege agrees that it will:
a. not "sell" or "share" such Personal Information, nor Process it for purposes of "targeted advertising" (as such terms are defined under applicable US State Privacy Laws);
b. not retain, use, or disclose such Personal Information for any purpose—including any commercial purpose—that is not a business purpose set forth in the Agreement, or as otherwise permitted under applicable US State Privacy Laws;
c. not retain, use, or disclose such Personal Information outside of the direct business relationship between Company and Prodege;
d. not combine such Personal Information 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 the Data Subject, except where permitted under applicable US State Privacy Laws;
e. provide the same level of privacy protection as is required under US State Privacy Laws;
f. notify Company if Prodege determines it can no longer meet its obligations under this section; and
g. allow Company to take reasonable and appropriate steps to stop and remediate the unauthorized Processing of such Personal Information.

iii. User Data. With respect to the Processing of User Data that contains Personal Information subject to US State Privacy Laws, the Parties agree that:

a. Data Subjects' use of Prodege to intentionally disclose such User Data to Company (or a third party at Company's direction) will position Company as an independent Controller with respect to that data under applicable US State Privacy Laws.
b. Notwithstanding any provision of this DPA to the contrary, in Processing any such Personal Information, Company will:
    1. only Process User Data for the limited and Specified Purposes set forth in the Agreement and this DPA;
    2. not "sell" or "share" Personal Information, or Process Personal Information for purposes of "targeted advertising" (as such terms are defined under applicable US State Privacy Laws), unless expressly authorized as a Specified Purpose and conducted in compliance with applicable law;
    3. promptly honor any consumer rights requests communicated by Prodege, the Data Subject directly, or via a legally recognized universal opt-out mechanism;
    4. comply with applicable US State Privacy Laws, including providing the same level of privacy protection for User Data as is required of a Controller;
    5. notify Prodege in the event Company determines it can no longer meet its obligations under applicable US State Privacy Laws; and
    6. permit Prodege to take reasonable and appropriate steps to: (i) ensure Company uses User Data in accordance with applicable US State Privacy Laws and this DPA; and (ii) stop and remediate any unauthorized Processing by Company, upon notice.

iv. Deidentified Data. To the extent either Party receives deidentified data from the other Party, or creates deidentified data from the US Personal Information it receives from the other Party, 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).

v. 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 E(v) and cooperate in making any required disclosures to U.S. authorities.

F. **Additional Terms for European Data**.

i. Scope of Application. This Section F applies solely to the extent that Personal Information Processed under the Agreement is subject to European Data Protection Laws, including where Data Subjects are located in Europe or where such laws otherwise apply to the

Processing, and such Personal Information is transferred outside Europe to a Third Country (an "**International Data Transfer**").

ii. Data Privacy Framework. Prodege participates in and certifies compliance with the Data Privacy Framework. Where and to the extent the Data Privacy Framework applies to the International Data Transfer, Prodege will (i) provide at least the same level of protection to the Personal Information as is required by the DPF Principles; and (ii) inform Company if Prodege determines that it is unable to comply with this requirement.

iii. Standard Contractual Clauses. In addition, the Parties agree that the EU Standard Contractual Clauses and UK Addendum will be incorporated by reference as set forth below and form an integral part of the Agreement. In the event any subsequent version of the EU Contractual Clauses or UK Addendum is adopted that is applicable to the Services, the Parties agree that the then-current version of the clauses will apply, in which case any references in this DPA to specific clauses of the EU Contractual Clauses or UK Addendum shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.

iv. EEA Transfers. In relation to Personal Information subject to the GDPR, the EU SCCs shall apply as follows:
   a. Module 1 shall apply to Controller-to-Controller ("**C2C**") transfers of User Data, Module 2 shall apply to Controller-to-Processor ("**C2P**") transfers of Company Data, and Module 4 shall apply to Processor-to-Controller ("**P2C**") transfers of Company Data;
   b. In all cases, Clause 7 (Docking Clause) is incorporated; the optional wording of Clause 11 (Redress) is excluded; Clause 17 (Governing Law) and Clause 18 (Jurisdiction) will reference Irish law and the Courts of Ireland; the competent supervisory authority will be the Irish Data Protection Commission; and Annex I is deemed completed with the information in Appendix 1 to this DPA;
   c. For C2C transfers, Annex II is completed with the relevant information provided by Company to Prodege;
   d. For C2P transfers, Clause 9(a) (Subprocessors) applies with "General Written Authorisation" selected and notifications will be made in accordance with Section C(v) of this DPA; and Annex II is completed with the information in Appendix 2.

v. UK Transfers. In relation to Personal Information subject to the UK GDPR, the EU SCCs will apply as set forth above and modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement. Tables 1, 2, and 3 of the UK Addendum will be deemed completed with the information in Appendices 1 and 2 to this DPA, and Table 4 will be deemed competed so that neither party may terminate the UK Addendum. Any conflict between the terms of the EU SCCs and UK Addendum will be resolved in accordance with Sections 10 and 11 of the UK Addendum.

vi. Swiss Transfers. In relation to Personal Information subject to the Swiss FADP, the EU SCCs will apply as set forth above and with the following modifications: (i) references to Member

States shall refer to Switzerland; (ii) references to applicable data protection law or the GDPR shall refer to the Swiss FADP; (iii) references to the competent courts shall be the competent courts of Switzerland; and (iv) the competent supervisory authority in Annex I.C. shall be the Swiss Federal Data Protection and Information Commissioner.

G. **Effective Date and Termination.**

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

ii. This DPA will remain in effect until such time as:
   a. the Agreement is terminated, or all Services thereunder are completed, and:
      1. Company instructs Prodege to delete all Company Data; or
      2. Prodege otherwise does so in accordance with the Agreement and Company's instructions.

iii. The provisions of this 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.

[*Remainder of this page intentionally left blank*]

APPENDIX 1

A. LIST OF PARTIES

1. Prodege:

Name: Prodege, LLC, or its affiliate, as identified in the Agreement

Address: 2030 E. Maple Ave, Suite 200, El Segundo, CA 90245, USA

Contact person's name, position and contact details:

Stacey Olliff, SVP, Legal and Business Affairs, dpo@prodege.com

Activities relevant to the data transferred under these Clauses:

The activities specified in the Agreement and in section B of this Appendix.

Signature and date: By executing the Agreement and/or this DPA, Prodege will be deemed to have signed this Appendix I.

Role:

- Module 1 (C2C): Controller and data exporter
- Module 2 (C2P): Processor and data importer
- Module 4 (P2C): Processor and data exporter

2. Company:

Name: As specified in the Agreement

Address: As specified in the Agreement

Contact person's name, position and contact details: As specified in the Agreement

Activities relevant to the data transferred under these Clauses:

The activities specified in the Agreement and in section B of this Appendix.

Signature and date: By executing the Agreement and/or this DPA, Company will be deemed to have signed this Appendix 1.

Role:

- Module 1 (C2C): Controller and data importer
- Module 2 (C2P): Controller and data exporter
- Module 4 (P2C): Controller and data importer

B. DESCRIPTION OF TRANSFER

1. Categories of Data Subjects whose Personal Information is transferred:
   - Survey respondents and other end users of Prodege services and solutions
   - Company contact persons and representatives
2. Categories of Personal Information transferred:

   The Agreement specifies the categories of Personal Information transferred, which (for survey respondents and other end users of Prodege services and solutions) may include: real name, account name, login or other alias, email address, street/postal address, telephone number, date of birth, demographic information, IP address, device ID (including IMEI), MAC address, or other identifying personal information, and for Company contact persons, real name, professional contact details (including location, postal and email address, professional phone number), job title, and contact preferences.
3. Sensitive data transferred (if applicable) and applied restrictions or safeguards:

   As specified in the Agreement.
4. Frequency of transfer (e.g. whether the data is transferred on a one-off or continuous basis):

   As specified in the Agreement.
5. Nature of the processing:

   Collection, processing and/or transfer of EEA/UK/Swiss data subjects' Personal Information on behalf of Company, as specified in the Agreement.
6. Purpose(s) of data transfer and further processing: (as applicable)
   - For Company's benefit in surveying respondents, and/or processing the Personal Information of other data subjects, as specified in the Agreement.
   - To perform services on behalf of Company, including: 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, reward value and quality of ad/survey impressions and completions; helping to ensure security and integrity; debugging to identify and repair errors; internal research for technological development and demonstration; and verifying or maintaining the quality or safety of the services.
   - To manage the contractual relationship with Company
7. Period for which Personal Information will be retained, or, if that is not possible, the criteria used to determine that period so long as necessary to achieve the purpose of the transfer:

   As specified in the Agreement, or for so long as necessary or permitted to achieve the purpose of the transfer.
8. For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:

   See Section C(v) of this DPA for details relating to authorized Subprocessors.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING MEASURES TO ENSURE THE SECURITY OF COMPANY DATA

Prodege has implemented and shall maintain the following technical and organizational security measures to protect Company Data, at a minimum:

1. Appropriate environmental and physical security measures to prevent unauthorized physical access to Company Data and the systems used to manage it;
2. Restricting access to only the resources necessary for users (application, database, network, and system administrators) to perform authorized functions, and documenting all the user types and their related permissions;
3. Requiring strong authentication and encryption that meet industry security standards for any remote access to Company Data or Prodege's network;
4. Securing authentication information (username and password) using recognized industry security standards;
5. Separating Prodege's information from any other customer or data importer's own applications and information, including but not limited to the public internet or any system used by the data importer;
6. Information is protected using appropriate tools and measures, including but not limited to access control, firewall and antivirus applications;
7. Prohibiting the transfer and storage of Company Data on removable devices, laptops, smartphones, tablets, etc., and implementing security measures such as encrypting information stored on mobile devices;
8. Regularly installing the most recent system and security updates to systems that are used to access, process, manage, or store Company Data;
9. Conducting risk assessment processes and surveys to regularly assess information security risks, and remediating any identified risks as soon as possible;
10. Employing appropriate identification and access controls to any of Prodege's systems and saving log files of all access to Company Data;
11. Transferring Company Data by using secure file transfer protocol via an industry-standard provider;
12. Conducting third-party penetration tests not less than annually;
13. Dedicated internal resource for periodic code review;
14. Ensuring that all personnel, subcontractors or representatives performing work under the Agreement act in compliance with these measures; and
15. Providing an appropriate level of periodic training concerning the organizational security measures and privacy issues, to personnel who have access to Company Data.