Data Sharing Agreement
for Offer Clients

This Data Sharing Agreement (**"DSA"**) for Offer Clients supplements, amends and forms part of the 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 client that has executed below and its affiliates (collectively, "**Company**") (each a "**Party**," and together, the "**Parties**"). Pursuant to the Agreement, Prodege provides certain services ("**Services**") that involve the exchange and transfer of "personal information" or "personal data", as such terms are defined under Data Protection Laws (collectively "**Personal Information**"), between the Parties. To the extent this DSA and the Agreement conflict with respect to any subject matter herein, this DSA will control, unless expressly agreed otherwise in writing.

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

   i. Application. This DSA applies to the extent that either Party transfers Personal Information to the other Party in connection with the Services, including where Company authorizes its third-party measurement partner to transfer Personal Information to Prodege. This DSA applies to the Processing of Personal Information of Data Subjects located anywhere, including in the United States and Europe.

   ii. Role of the Parties. Each Party will act as an independent Controller or Third Party (as such terms are defined under Data Protection Laws) of Personal Information. This means that each Party determines the purposes and means of Processing and is responsible for its own Processing of Personal Information in connection with the Agreement. Nothing in this DSA will modify any restrictions on either Party's rights to use or otherwise Process Personal Information under the Agreement.

   iii. Details of Processing. The subject matter, duration, nature, and purpose of the Processing, and the types of Personal Information and categories of Data Subjects, are set forth in **Appendix 1** to this DSA.

B. **Definitions**. This DSA 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. **"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.

   ii. **"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.

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means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded, or replaced.

iv. **"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.

v. **"Data Protection Laws"** means all data protection, privacy, and/or security laws, rules, and regulations that are now or may become applicable to Personal Information exchanged or transferred between the Parties pursuant to the Agreement during its term, including, without limitation, European Data Protection Laws and US State Privacy Laws, as amended, superseded, or replaced.

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

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

viii. **"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.

ix. **"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.

x. **"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.

xi. **"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.

xii. **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

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

xiv. **"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.

xv. **"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.

xvi. **"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.

xvii. **"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. **Undertakings of the Parties.** To the extent the Parties act as independent controllers of Personal Information, the following provisions apply:

i. Compliance with Law. Each Party represents and warrants that, with respect to any Personal Information it transfers to the other Party, it has and will maintain all necessary rights, consents, and authority for the other Party to Process Personal Information for the purposes specified in the Agreement and in compliance with applicable Data Protection Laws.

ii. Permitted Purposes. Each Party may Process Personal Information it receives from the other Party solely in accordance with any restrictions set forth in the Agreement and for the purpose(s) specified in the Agreement under which the data was made available (including, as applicable, targeting and delivering offers; measurement and attribution, including using tracking technologies; analytics and reporting; market segmentation; fraud prevention; and improvement and optimization) (collectively, the **"Specified Purposes"**).

iii. Security. Each Party will implement and maintain reasonable security procedures and practices to protect Personal Information it receives from the other Party, and will notify the other Party without undue delay if it becomes aware of a Security Incident which is likely to affect or invoke the other Party's obligations under Data Protection Laws.

iv. Cooperation. If either Party receives any complaint, notice, or communication from a Data Subject or authority which relates to the other Party's Processing of Personal Information, or potential failure to comply with Data Protection 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.

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

i. Scope of Application. This Section D 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. Third-Party Terms. Notwithstanding any provision of this DSA to the contrary, solely with respect to the Processing of Personal Information that is subject to US State Privacy Laws, each Party agrees that it will:

a. only Process it for the limited and Specified Purposes set forth in the Agreement and this DSA;
b. 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), unless expressly authorized as a Specified Purpose and conducted in compliance with applicable law;
c. promptly honor any consumer rights requests communicated by the other Party or the Data Subject directly;
d. comply with applicable US State Privacy Laws, including providing the same level of privacy protection for US Personal Information as is required under applicable US State Privacy Laws;
e. notify the other Party in the event that it can no longer meet its obligations under applicable US State Privacy Laws; and
f. permit the other Party to take reasonable and appropriate steps to: (i) ensure it uses Personal Information in accordance with applicable US State Privacy Laws and this DSA; and (ii) stop and remediate any unauthorized Processing, upon notice.

iii. 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).

iv. Covered Data Transactions. Company agrees not to direct, permit, or facilitate any Covered Data Transaction involving US Personal Information under the Agreement.

Company will notify Prodege within 72 hours of any known or suspected breach of this section D(iv) and cooperate in making any required disclosures to U.S. authorities.

E. **Additional Terms for European Data**.

i. Scope of Application. This Section E applies solely to the extent that Personal Information exchanged or transferred between the Parties 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 DSA 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;
   b. To the extent that Prodege transfers Personal Information to Company, then Prodege will be deemed to have entered into the EU SCCs as the data exporter with Company as the data importer;
   c. To the extent that Company transfers Personal Information to Prodege, then Company will be deemed to have entered into the EU SCCs as the data exporter with Prodege as the data importer;
   d. 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
   e. Annex I and Annex II are deemed completed with the information in Appendix 1 and Appendix 2 to this DSA.

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 Appendix 1and Appendix 2 to this DSA, 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.

F. **Effective Date and Termination.**

i. This DSA is effective as of the earlier of the date that Company either:
   a. executes the DSA; or
   b. enters into the Agreement incorporating it by reference.

ii. This DSA will remain in effect until such time as the Agreement is terminated or all Services thereunder are completed.

iii. The provisions of this DSA that are reasonably expected to survive termination (e.g., compliance with Data Protection Laws and security obligations) shall survive termination of the Agreement.

[*Remainder of 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 DSA, Prodege will be deemed to have signed this Appendix 1

Role: Data exporter and/or data importer

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 DSA, Company will be deemed to have signed this Appendix 1

Role: Data exporter and/or data importer

B. DESCRIPTION OF TRANSFER

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

2. Categories of Personal Information transferred:

The categories of Personal Information transferred for offer participants and other end users of Prodege services and solutions may include: IP address, device ID (including IMEI), user ID, device data, usage event information (including game play and in-app purchases), and other identifying Personal Information. The categories of Personal Information transferred for Company contact persons may include: 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:

   N/A

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

   Continuous.

5. Nature of the processing:

   Collection, processing and/or transfer of Personal Information to facilitate offers, as specified in the Agreement.

6. Purpose(s) of data transfer and further processing: (as applicable)
   - For Company's benefit in facilitating user acquisition and engagement, as specified in the Agreement.
   - Targeting, personalizing, and facilitating offers and user experiences.
   - Hosting, advertising, optimizing, and analyzing offers and their performance.
   - Auditing the amount, positioning, reward value and quality of ad/offer impressions and completions.
   - Maintaining or servicing accounts; billing and payment processing; providing customer service; and verifying information.
   - Helping to ensure security and integrity; debugging to identify and repair errors; maintaining the quality or safety of the services.
   - Analytics to maintain and improve the services; internal research for technological development and demonstration;
   - 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.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING MEASURES TO ENSURE THE SECURITY OF PERSONAL INFORMATION

The Parties shall implement and maintain the following technical and organizational security measures to protect Personal Information, at a minimum:

1. Appropriate environmental and physical security measures to prevent unauthorized physical access to Personal Information 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 Personal Information;
4. Securing authentication information (username and password) using recognized industry security standards;
5. Separating Personal Information from any other data importer's own applications and information, including but not limited to the public internet or any system used by the data importer;
6. Personal 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 Personal Information 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 Personal Information;
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 company systems and saving log files of all access to Personal Information;
11. Transferring Personal Information 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 Processing Personal Information 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 Personal Information.