# Prodege Market Research
# Data Protection Addendum

1. Data Processing. This Data Protection Addendum (**DPA**)—when incorporated by reference therein—automatically supplements, amends and forms part of any present or future master services agreement (MSA), statement of work, insertion order (IO), or other written business understanding (collectively, the "**Agreement**") between Prodege, LLC and its affiliates ("**Prodege**") and the Prodege market research client that is counterparty to that Agreement and its affiliates ("**Company**") (each a "Party" and collectively, the "Parties"). Pursuant to the Agreement, Prodege may provide market research services for or on behalf of Company ("**Services**") involving the Processing of "personal information" or "personal data"—as these terms are defined under applicable US, EU/EEA, UK, Swiss and Australian data privacy and/or protection laws—that is provided by Company or collected by Prodege on Company's behalf ("**Company Data**").

2. Definitions. The following definitions shall apply for purposes of interpreting this DPA. Capitalized terms used but not defined in this DPA have the meaning given to them in the Agreement or Data Protection Laws.

   a) "**Breach**" means a security incident affecting Prodege's Processing of Company Data that requires notification to data subjects and/or government authorities under Data Protection Laws.

   b) "**Business Purposes**" means the enumerated Business Purposes set forth in Cal. Civ. Code section 1798.140(d)(1)-(7) and, on or after January 1, 2023, Cal. Civ. Code section 1798.140(e)(1)-(8) that are applicable to the Services as set forth in the Agreement, including but not limited to: performing Services on behalf of Company, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of Company.

   c) "**Consumer Rights Request(s)**" means a communication from a consumer or other data subject requesting to exercise their individual privacy rights under the GDPR, UK GDPR, US Privacy Laws, or other applicable Data Protection Laws.

   d) **"Data Protection Law(s)"** means all applicable laws which govern the use of data and privacy relating to identified or identifiable individuals, including, among others, the GDPR (and any implementing legislation), the Data Protection Act 2018, U.S. Privacy Laws, the Privacy Act, and Directive 2002/58/EC (known as the e-Privacy Directive) (and any implementing legislation), as amended or replaced from time to time and to the extent applicable to a Party.

   e) **"EU Standard Contractual Clauses" or "Approved EU SCCs"** means, where the GDPR or Swiss DPA applies, the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version thereof released by the European Commission. In the event any subsequent version of such clauses is released 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 shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.

   f) **"GDPR"** means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

g) **"Privacy Act"** means the *Privacy Act 1988* (Cth) and any regulations and guidance that may be issued pursuant to the Privacy Act from time to time.

h) "**Swiss DPA**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

i) **"Third Country(ies)"** means any country that is neither a member of the European Economic Area ("**EEA**") or United Kingdom ("**UK**") nor has an adequacy status (i.e. (i) a status granted by the European Commission to non-EEA countries which provide a level of personal data protection that is comparable to that provided in EU law in accordance with GDPR, or (ii) a status granted by UK Secretary of State to non-UK countries which provide a level of personal data protection that is comparable to that provided in UK law in accordance with UK Data Protection Laws).

j) **"UK Addendum"** means the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

k) **"UK Data Protection Laws"** means the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law ("**UK GDPR**"), as amended, and any other applicable UK data protection laws.

l) **"US Privacy Law(s)"** means all applicable U.S. federal and/or state security, confidentiality, and/or privacy laws, and regulations that are applicable to Prodege, the Services, Company Data, and/or any other programs or products provided pursuant to the Agreement, including but not limited to the California Consumer Privacy Act as amended by the California Privacy Rights Act (collectively, the "**CCPA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, and any implementing regulations thereunder, in each case applicable to this DPA as and when legally effective.

3. Restrictions on Prodege's Processing: Prodege is permitted to Process Company Data solely for purposes of performing the Services and to carry out the Business Purposes under the Agreement, or as otherwise required or permitted by Data Protection Laws of a Service Provider/Processor, or as agreed to or instructed by Company. Without limiting the generality of the foregoing, except as otherwise permitted by the forgoing sentence, Prodege is prohibited from:

   a) Selling or Sharing Company Data;
   b) retaining, using, disclosing, or otherwise Processing Company Data for any purpose other than for the specific purpose of providing Services to Company and to carry out the Business Purposes under the Agreement;
   c) retaining, using, or disclosing Company Data for any commercial purpose other than to perform the Services and to carry out the Business Purposes under the Agreement;
   d) retaining, using, disclosing, or Processing Company Data outside of the direct business relationship between Company and Prodege; and
   e) on or after January 1, 2023, combining Personal Information received from or on behalf of Company with Personal Information it receives from, or on behalf of, another person(s), or collects from its own interaction with a consumer, except where expressly required to perform the Services.

Prodege certifies that it understands, and will comply with, the restrictions in this Section 3. Prodege will not permit any third party to access to Company Data, unless agreed to or instructed by Company or required by Data Protection Laws, except that Prodege may use subcontractors to perform the Services, provided (i) Prodege provides Company a reasonable opportunity to object to the engagement of subcontractors; and (ii) such subcontractors agree in writing to the same terms that apply to Prodege through this DPA.

Notwithstanding anything herein to the contrary, Company acknowledges that Prodege may retain, use, disclose, or otherwise Process Company Data in manners permitted of a Service Provider/Processor or as otherwise required by Data Protection Laws (e.g., to engage subcontractors for sub-processing, for permitted internal uses such as improving products and services, for security and fraud prevention, compliance with legal obligations, etc.) and may create Deidentified data and Aggregate Consumer Information from Company Data subject to Section 4(a) below ("**Permitted Vendor Purposes**"). Notwithstanding the foregoing, with respect to Company Data which Processing is subject to the GDPR, UK GDPR, or the Swiss DPA, Permitted Vendor Purposes are limited to Anonymized data. Company represents and warrants that it has informed the Company Data data subjects that their Personal Data is subject to Anonymization by third parties.

4. Prodege's Obligations: Prodege shall, with respect to the Services and the Company Data:
   a) to the extent Prodege receives, or Prodege creates, Deidentified data in connection with this DPA: (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 to attempt to reidentify the information; (iii) not attribute Company as a source of such data; and (iv) contractually obligate any third parties receiving such information from Prodege to also commit to (i), (ii), and (iv);
   b) comply with Data Protection Laws in performing the Services, reasonably assist Company in meeting its obligations under Data Protection Laws, and make available to Company information in Prodege's possession necessary to demonstrate compliance with its obligations under Data Protection Laws upon Company's reasonable request (subject to time and materials charges at standard rates if material efforts are required);
   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) ensuring each person Processing Company Data is subject to a duty of confidentiality with respect to such Company Data;
   d) notify Company if it 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;
   e) upon Company's request, provide reasonable assistance to enable Company to fulfill data subject access requests ("**DSARs**") (subject to time and materials charges at standard rates if material efforts are required), including but not limited to notifying Prodege's subcontractors to delete Company-specified Company Data in response to a DSAR made to Company. Company shall inform Prodege of DSARs that it needs Prodege's assistance to comply with and shall provide Prodege with information necessary to assist Company to comply with such DSARs;
   f) if Prodege receives a DSAR from a data subject that might relate to Company Data it shall respond that it cannot act upon requests made to it as to data it Processes as a Service Provider/Processor. If the request specifically identifies Company in connection with the DSAR, Prodege shall inform Company of such request;
   g) notify Company of a Breach and provide reasonable assistance and information regarding such Breach (as it may be required for the purposes of reporting to the authorities and, where necessary, to the data subjects);
   h) provide Company information to reasonably enable it to conduct and document data protection assessments and prior consultations to the applicable supervisory authority;

i) delete Company Data at the end of the provision of Services, or as otherwise instructed by Company or agreed in the Agreement, unless retention is (i) required by Data Protection Laws; or (ii) retained as part of backup or record keeping, so long as only used for such purposes and only for as long as reasonably necessary, subject to Data Protection Laws and this DPA;
j) allow Company to take reasonable and appropriate steps to ensure Prodege is using Company Data consistent with Company's obligations under Data Protection Laws; and
k) make available to Company information necessary to demonstrate compliance with its obligations under the Data Protection Laws and not more than once annually (to the extent permitted by Data Protection Laws), allow and cooperate with reasonable assessments by Company, or its designated assessor (or if mutually agreed and at Prodege's expense, Prodege's qualified assessor), to conduct a reasonable assessment of Prodege's policies and technical and organizational measures in support of the obligations under Data Protection Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments and subject to reasonable access and confidentiality restrictions. If Prodege engages its own assessor, it shall provide a report of such assessment to Company upon request. If Prodege receives instructions from Company that, in its opinion, infringe Data Protection Laws, it shall immediately inform Company about it. Any assessments shall be subject to Prodege's reasonable access and confidentiality requirements.

5. Company Obligations: Company represents and warrants that any Company Data collected by Company has been collected in accordance with Data Protection Laws and is transferred to Prodege in connection with this DPA in accordance with Data Protection Laws. Company acknowledges that it is the Controller of Company Data and shall take all steps necessary to ensure that it has all necessary authority and Consent to enable Prodege to use the Company Data to provide the Services and Process Company Data consistent with Data Protection Laws, the Agreement, and this DPA, including without limitation timely providing Prodege all instructions for Prodege's Processing as may be required by Data Protection Laws (e.g., notice to delete, notice to discontinue certain processing, etc.).

6. International Data Transfers: For data transfers from the EEA/UK to Third Countries, to the extent such transfers are subject to GDPR (including the UK GDPR) and/or the Swiss DPA, the Parties hereby incorporate the EU Standard Contractual Clauses and/or the UK Addendum as follows:

   a) If Company is located in the US and requests Company Data transferred from Prodege to Company, Exhibit A will apply.

7. Compliance with the Privacy Act: To the extent that the Privacy Act applies to Company Data Processed by Prodege or disclosed to Prodege in accordance with this DPA and without limiting any other provision of this DPA:
   a. Prodege shall comply with the Australian Privacy Principles (other than Australian Privacy Principle 1) contained within the Privacy Act in relation to the collection, use, disclosure, storage and destruction or de-identification of such Company Data; and
   b. Company shall, on behalf of Prodege, provide notice of Prodege's collection of Company Data to any individual in Australia or such other individual who is otherwise entitled to exercise rights under the Privacy Act and whose personal information comprises Company Data to a standard reasonably consistent with Prodege's obligations pursuant to Australian Privacy Principle 5.

[*Remainder of page intentionally left blank*]

# Exhibit A

## STANDARD CONTRACTUAL CLAUSES

Module 4 [Processor to Controller]

**SECTION I**

***Clause 1***
**Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:
   (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***Clause 2***
**Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3***
**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8.1 (b) and Clause 8.3(b);
   (iii) N/A
   (iv) N/A

(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4***
**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6***
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7 – Optional***
**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### 8.2 Security of processing

(a) The Parties shall implement appropriate technical and organizational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. With respect to Prodege as data exporter, as of the effective date of this DPA Prodege has implemented the technical and organizational measures described in Annex II.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

***Clause 9***

**Use of sub-processors**

N/A

***Clause 10***

**Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

***Clause 11***

**Redress**

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

***Clause 12***

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

N/A

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

### *Clause 14*

### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

### Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

### Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

### *Clause 18*

### Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

## APPENDIX

## ANNEX I

### A. LIST OF PARTIES

**1. Data exporter(s):**

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

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

**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 Annex.

**Signature and date**: By signing the DPA and/or transferring Company Data to Third Countries on Company's instructions, the data exporter will be deemed to have signed this Annex I.

**Role**: Processor

**2. Data importer(s):**

**Name**: As specified in the Agreement, as the same may be amended from time to time (which amendment shall serve to update this Section B), if applicable.

**Address**: As specified in the Agreement, as the same may be amended from time to time (which amendment shall serve to update this Section B), if applicable.

**Contact person's name, position and contact details**:

As specified in the Agreement, as the same may be amended from time to time (which amendment shall serve to update this Section B), if applicable.

**Activities relevant to the data transferred under these Clauses**:

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

**Signature and date**: By signing the DPA and/or using the Services to transfer Company Data to Third Countries, the data importer will be deemed to have signed this Annex I.

**Role**: Controller

## B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Survey respondents

Categories of personal data transferred: The Agreement, as the same may be amended from time to time (which amendment shall serve to update this Section B), specifies the categories of personal data transferred, which may include real name, account name, login or other alias, email address, street/postal address, telephone number, date of birth, demographic information, government ID number or image, IP address, device ID (including IMEI), MAC address, or other identifying personal information.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

As specified in the Agreement, as the same may be amended from time to time (which amendment shall serve to update this Section B), if applicable.

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

One-time upon completion of the project(s) described in the Agreement or on a continuous basis for the term of the Agreement.

Nature of the processing:

Onward transfer of EU data subjects' personal data.

Purpose(s) of the data transfer and further processing:

For the client/controller's benefit in obtaining survey respondents' personally identifiable information.

The period for which the personal data 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 so long as necessary to achieve the purpose of the transfer.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:

N/A

## ANNEX II

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

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

1. Appropriate environmental and physical security measures to prevent unauthorized physical access to restricted information and the systems managing 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 security standards for any remote access to confidential information and Prodege's network;
4. Securing authentication information (username and password) only by acceptable 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 Prodege's 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 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 of Prodege's systems and saving log files of all access to confidential information;
11. Transferring confidential 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 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 the personnel who have access to Prodege's confidential information.

**LIST OF PRE-APPROVED SUB-PROCESSORS**

Company has authorized the use of the following sub-processors of Prodege:

1.

Name: Amazon Web Services

Address: 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.

Contact person's name, position and contact details: N/A

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):

Cloud data storage

2.

Name: Forsta/Decipher

Address: c/o Confirmit, Inc., 330 Seventh Avenue, 3rd floor, New York, NY 10001 United States

Contact person's name, position and contact details: Bob Hull, Vice President (North America); info@forsta.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):

Survey hosting services