



DATA PRIVACY ADDENDUM

THIS DATA PRIVACY ADDENDUM (“DPA”) is made as of _____, 20__ by and between TEKNIK TRADING, LLC (“Company”) and _____ (“Customer”).

RECITALS:

A. Company and Customer have entered into that certain Services Agreement, dated _____, pursuant to which Company provides certain relationship management, processing, logistics, and similar services. Such agreement is referred to herein as the “Agreement”;

B. To carry out its obligations under the Agreement, Company may have access to and be required to hold, collect, organize, record, structure, store, adapt, alter, retrieve, consult, use or process certain personal data controlled by Customer; and,

C. Customer and Company desire to make this Addendum to the Agreement in order to ensure compliance with certain data privacy laws, including but not limited to the European Union General Data Protection Regulation 2016/679 and related regulations and directives.

NOW, THEREFORE, for and in consideration of the mutual promises herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

I. DEFINITIONS

Capitalized terms used in this Addendum and not otherwise defined herein shall have that meaning given to them in the Agreement.

1.1 “Affiliate” means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with an entity, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 “Applicable Laws” means (a) European Union or Member State laws with respect to any Personal Data in respect of which any Company Group Member is subject to EU Data Protection laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws.

3. 1.3 “Group Member” means Company or any Company Affiliate.

4. 1.4 “Customer Personal Data” means any Personal Data Processed by a Contracted Processor

on behalf of a Company Group Member pursuant to or in connection with the Agreement.

1.5 “Contracted Processor” means Company or a Sub-processor.

1.6 “Customer Data” means any Personal Data that Company processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.



1.7 “Data Controller” means an entity that determines the purposes and means of the processing of Personal Data.

1.8 “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country or Member State.

1.9 “Data Processor” means an entity that processes Personal Data on behalf of a Data Controller.

1.10 “EU Data Protection Law” means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive") and on and after May 25, 2018, Regulation 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 (General Data Protection Regulation) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

1.11 “EEA” means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

1.12 “GDPR” means EU General Data Protection Regulation 2016/679.

1.13 “Personal Data” means any information relating to an identified or identifiable natural person.

1.14 “Privacy Shield” means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by European Commission pursuant to Decision C(2016)4176 of July 12, 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

1.15 “Privacy Shield Principles” means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded or replaced).

1.16 “Processing” has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly.

1.17 “Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

1.18 “Services” means the services and other activities to be supplied to or carried out by or on behalf of Company for Customer pursuant to the Agreement.

1.19 “Sub-processor” means any person (including any third party and any Company Affiliate, but excluding an employee of Company) appointed by or on behalf of Company or any Company Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Agreement.

1.20 “Company Affiliate” means an entity that owns or controls, is owned or controlled by or is under common control or ownership with Company, where control is defined as the possession, directly or



indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.21 The terms Commission “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing”, “Processor”, and “Supervisory Authority” shall have the same meaning as in the GDPR and such terms shall be construed accordingly.

II. RECITALS AND GENERAL PROVISIONS

2.1 Recitals. The recitals to this DPA are hereby incorporated into this DPA.

2.2 Prior Agreement / Enforceability and Conflict. The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict. Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.3 Claims / Liability of Parties. Any claims against Company or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by Company in relation to the Customer Data that arise as a result of or in connection with Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Company's liability under the Agreement as if it were a liability to the Customer under the Agreement.

2.4 Applicability. This DPA applies where and only to the extent that Company processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

III. ROLES OF PARTIES

3.1 Role of the Parties. As between Company and Customer, Customer is the Data Controller of Customer Data, and Company is the Data Processor that shall process Customer Data on behalf of Customer. Company may hire Sub-processors as set forth herein.

3.2 Customer Processing of Customer Data. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any Processing instructions it issues to Company; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Company to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

3.3 Company Processing of Customer Data. Company shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Company in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Company.



IV. PROCESSING OF PERSONAL DATA

4.1 Details of Data Processing.

(a) Subject Matter / Duration / Purpose. The subject matter of the data processing under this DPA is the Customer Data. As between Company and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms. The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Company's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(b) Nature of the processing. Company provides a service that allows Customers to store, retrieve, organize and share data related to current and prospective advertisers or subscribers, as well as other related services, as described in the Agreement.

(e) Data Subjects and Types of Customer Data. Data of current and prospective advertisers and subscribers is collected by Customers. "Users" shall be any such current or prospective advertiser or subscriber (or other individual): (i) whose information is stored on or collected via the Services, or (ii) to whom Customers send emails or otherwise engage or communicate with via the Services.

(f) Categories of User Data. The following types of User Data (some or all of which may be Personal Data) will be collected: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including phone number and/or email address), personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information); order history, quotation history, notes of phone calls and meetings held, copies of email correspondence received, and billing information.

4.2 Company Rights to Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Company shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, Company is the Data Controller of such data and accordingly shall process such data in accordance with the Company Privacy Policy and Data Protection Laws.

4.3 Tracking Technologies. Customer acknowledges that in connection with the performance of the Services, Company employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable Company to deploy Tracking Technologies lawfully on, and collect data from, the devices of Subscribers (defined below) in accordance with and as described in the Company Cookie Statement.



V. SUBPROCESSING

5.1 Authorized Sub-processors. Customer agrees that Company may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Company and authorized by Customer are listed in Schedule 1.

5.2 Sub-processor Obligations. Company shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Company to breach any of its obligations under this DPA.

VI. SECURITY / SECURITY REPORTS AND AUDITS

6.1 Security Measures. Company shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Company's security standards described in Schedule 2 ("Security Measures").

6.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Company relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

6.4 Security Reports and Audits. Customer acknowledges that Company's data hosting Sub-processors are regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors, respectively. Upon request, Company shall supply (on a confidential basis) a summary copy of such audit report(s) ("Report") to Customer, so that Customer can verify Company's Sub-processors' compliance with the audit standards against which it has been assessed, and this DPA. Company shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm Company's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

6.5 International Transfers. Company may transfer and process Customer Data anywhere in the world where Company, its Affiliates or its Sub-processors maintain data processing operations. Company shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.



VII.

ADDITIONAL SECURITY / CHANGES TO SUB-PROCESSORS RETURN OR DELETION OF DATA / COOPERATION

7.1 Confidentiality of processing. Company shall ensure that any person who is authorized by Company to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

7.2 Security Incident Response. Upon becoming aware of a Security Incident, Company shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

7.3 Changes to Sub-processors. Company shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email or published notification on Company's website shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes. Customer may object in writing to Company's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination) but only if Customer's objection is based on reasonable and specified grounds relating to data protection.

7.4 Return or Deletion of Data. Upon termination or expiration of the Agreement, Company shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Company is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Company shall securely isolate and protect from any further processing, except to the extent required by applicable law.

7.5 Cooperation. The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Company shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Company, Company shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. If a law enforcement agency sends Company a demand for Customer Data (for example, through a subpoena or court order), Company shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Company shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. To the extent Company is required under EU Data Protection Law, Company shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.



VIII. TERM AND TERMINATION

8.1 Term. The Term of this DPA shall be effective as of the date first written above and shall expire upon the expiry of the Agreement; provided, however, that the DPA shall remain in full force and effect to the extent that any party hereto must destroy or return Customer Personal Data, or, if it is infeasible, to return or destroy Customer Personal Data.

8.2 Termination. Upon either Customer's or Company's (the "non-breaching party") reasonable knowledge of a material breach by the other party ("the breaching party") of its obligations under this DPA, such party shall: (i) provide reasonable written prior notice to the breaching party of the alleged breach under the DPA, (ii) provide an opportunity for the breaching party to cure the breach or otherwise terminate the Agreement and this DPA without penalty, (iii) in the event such breaching party does not cure the alleged breach within a reasonable amount of time, or terminate this DPA and the Agreement, and the non-breaching party's determination of the existence of a material breach by Company was reasonable, terminate this DPA and the Agreement without penalty, or (iv) immediately terminate, without penalty, this DPA and the Agreement if the breaching party has breached a material term of this DPA and cure is not possible; or (v) if neither termination nor cure are feasible, report the violation to the Supervisory Authority.

8.3 Return or Destruction of Protected Health Information Upon Termination. Within thirty (30) days of the date of termination of the Agreement or the date of cessation of any Services involving the Processing of Customer Personal Data, Company shall delete, destroy and procure the deletion of all copies of such Customer Personal Data. Customer may in its sole and absolute discretion request by written notice a complete copy of all Customer Personal Data prior to deletion and destruction of such data by Company. Company shall provide written certification to Customer that it and each Company Affiliate has fully complied with this Section 4.3 within thirty (30) days of the termination of Agreement or date of cessation of Services.

IX. MODIFICATIONS

The parties agree and acknowledge that Data Protection Laws including but not limited to GDPR include provisions that impose additional requirements on Processors and Controllers (as those terms are defined in the GDPR). Accordingly, Customer and Company agree that any provisions of the Data Protection Laws that apply to Processors and that are required to be incorporated by reference in an agreement are incorporated into this Addendum as if set forth in this Addendum in their entirety and are effective as of the applicable effective date for each such provision. In the event that additional rules are promulgated under the Data Protection Laws, or any existing rules are amended, the parties agree to enter into a mutually acceptable amendment to this Addendum to enable a Company and/or Customer to satisfy its obligations under such additional or amended rule(s). Either Customer or Company, as the case may be, may terminate this Agreement in the event the same are unable to enter into a mutually acceptable amendment to this Addendum or the Agreement that would enable either party to satisfy its obligations under such additional or amended rule(s).

X. MISCELLANEOUS

10.1 Regulatory References. A reference in this Addendum to a section in a regulation or Applicable Law means the section as in effect or as amended.



10.2 Governing Law. Unless required otherwise by applicable Data Protection Laws, this DPA shall be governed by and construed in accordance with the law of the State of Florida and the parties agree that the venue for any disputes relating to this DPA shall be a court of competent jurisdiction in Broward County, Florida.

10.3 Survival. The respective rights and obligations of Company and Customer as set forth in this Addendum shall survive the termination or expiration of this Addendum.

10.4 Interpretation; Entire Agreement; Amendment. The headings of sections in this Addendum are for reference only and shall not affect the meaning of this Addendum. Any ambiguity in this Addendum shall be resolved to permit the Company and/or Customer to comply with relevant Applicable Laws. This Addendum, together with the Agreement, constitutes the entire agreement between the parties regarding the subject matter herein. This Addendum may be amended only by written agreement between the parties.

10.5 Severability. In the event any provision of this Addendum is held to be invalid, illegal or unenforceable for any reason and in any respect, such invalidity, illegality, or unenforceability shall in no event affect, prejudice, or disturb the validity of the remainder of this Addendum, which shall be and remain in full force and effect, enforceable in accordance with its terms.

10.6 No Third Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors and assigns of the parties any rights, remedies, obligations, or liabilities whatsoever.

IN WITNESS WHEREOF, the parties hereto have executed this Addendum as of the day and year first written above.

COMPANY:

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER:

By: _____

Name: _____

Title: _____

Date: _____

