

## DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is made part of the Publisher Services Agreement (“Agreement”) entered into by and between Marathon Ventures, LLC (“Agency”), and the company defined as “Publisher” therein. In the event of any conflict between this DPA and the Agreement, the provision of this DPA will control. Any capitalized terms used, but not otherwise defined herein shall have the meaning set forth in the Agreement. By executing the Agreement, the parties agree to the terms of this DPA.

### 1. Definitions.

a. **“Data Protection Law”** means any laws, rules, or regulations relating to privacy, security, or data protection applicable to a party in the performance of its obligations under this DPA, including, as applicable the California Consumer Protection Act, as amended (“CCPA”); (ii) those of the European Union, the European Economic Area, their member states, and the United Kingdom, including Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (“GDPR”), the UK Data Protection Act 2018 as saved into United Kingdom law by virtue of Section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018 (“UK GDPR”), and the Swiss Federal Data Protection Act; (iii) those of any other relevant jurisdictions; and (iv) any replacements, additions, successors, implementing requirements or legislation, or amendments to any of the foregoing.

b. **“Data Subject”** means a data subject, consumer, or identified or identifiable natural person.

d. **“Personal Data”** means any data that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject or household, or that is personal data, personal information, or similarly protected data as ascribed under Data Protection Law.

g. **“Subprocessor”** means any subcontractor engaged directly by Agency to generally help provide services to Agency and that processes Personal Data on behalf of Agency in connection with Publisher’s use of the Services.

g. **“Vendor”** means any third party engaged at the direction and for the benefit of Publisher pursuant to the Agreement, including advertisers, ad networks, DMPs, DSPs, SSPs, technology platforms, social networks, and data providers.

Where applicable, the terms **“controller,” “business,” “processor,” “service provider,” “data subject,” “consumer,” “process,” “personal data,” “personal information,” “sell,” “share,” “business purpose,” “commercial purpose,” “supervisory authority,” “third party,” “deidentified,” “aggregate consumer information”** (or any equivalent terms) shall have the meaning ascribed to them under Data Protection Law.

2. Data Processing.

a. This DPA applies to the processing of Personal Data by Agency in connection with the Services. In this context, with respect to Personal Data (i) Agency acts as processor, service provider, or third party for Publisher; and (ii) Publisher acts as controller.

b. Publisher hereby instructs Agency to process Personal Data in accordance with (i) the Agreement and this DPA (including the details of data processing set out in **Schedule 1**); and (ii) any other documented written instructions by Publisher (e.g., via email) where such instructions are consistent with the terms of the Agreement and this DPA (collectively, "**Documented Instructions**"). If Agency must process Personal Data as otherwise required by applicable law, Agency shall inform Publisher of that legal requirement before processing Personal Data, unless that law prohibits such disclosure on important grounds of public interest.

c. The obligations in this subsection apply only to Personal Data that is personal information subject to the CCPA. Publisher makes Personal Data available to Agency for the limited purposes specified in the Agreement and this DPA. Agency agrees that: (1) Agency will use the Personal Data only for those limited specified purposes; (2) Agency will provide the same level of privacy protection to the Personal Data as is required of businesses by CCPA; (3) Publisher has the right to take reasonable and appropriate steps as outlined in Section 9 of this DPA to help ensure that Agency uses the Personal Data in a manner consistent with Publisher's obligations under CCPA; (4) Agency will notify Publisher if it makes a determination that it can no longer meet its obligations under CCPA with respect to the Personal Data; and (5) Publisher has the right, upon notice and in accordance with the applicable sections of this DPA, to take reasonable and appropriate steps to stop and remediate unauthorized use of the Personal Data. Publisher will promptly notify Agency of any requests received by Publisher from consumers to opt-out of the sale or sharing of their Personal Data which may impact Publisher's use of the Services. Upon receiving notice of a consumer request to opt-out of the sale or sharing of their Personal Data, Agency will only continue to process such Personal Data as permitted of a service provider under CCPA. Where Agency acts as a service provider, Agency further agrees that it will only process the Personal Data for the business purposes specified in Annex I and that Agency will not: (i) sell or share the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose, including a commercial purpose, other than the business purposes specified herein; (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between Agency and Publisher other than for the business purposes specified herein; or (iv) combine the Personal Data with personal information that Agency receives from or on behalf of another customer, or collects from its own interaction with the consumer, unless otherwise permitted of a service provider by the CCPA.

d. As between the parties, Publisher is solely responsible for the accuracy, quality, and legality of Personal Data. Publisher will provide and maintain on its online services (i) a privacy policy that accurately discloses Publisher's data practices relating to Personal Data it processes in connection with the Services, including an explanation of the use of cookies and other tracking technologies for purposes of targeted advertising; and (ii) links to functional consent/opt-out mechanisms that allows Data Subjects to opt out of sales, shares, or processing of Personal Data for purposes of targeted advertising. Publisher will be responsible for obtaining any consents required relating to the use of cookies and other tracking technologies in connection with the Services, regardless of whether technologies are set directly by Publisher, Agency, or otherwise. Publisher agrees that: (i) Publisher has provided all necessary notice and choice, and secured all necessary rights, consents, privileges, and a lawful basis for the processing of Personal Data as contemplated under the Agreement (including by Agency, its Subprocessors, and any Vendors);

(ii) Publisher has complied (and will continue to comply) with all Data Protection Laws and third party terms; (iii) Publisher will not provide to Agency or cause Agency to process any sensitive category of Personal Data (such as data concerning health, finances, sex life or sexual orientation, children or teens, or other data defined as sensitive or a special category of data under Data Protection Law) or Personal Data relating to Data Subjects located outside the United States unless expressly set out in the Agreement and Schedule 1 below; and (iv) Agency's processing of Personal Data in accordance with Publisher's instructions will not violate or cause Agency to violate any Data Protection Laws or third party terms. If the processing of any sensitive category of Personal Data or Personal Data relating to Data Subjects outside the United States is expressly authorized, the parties will negotiate in good faith additional terms to address such data, and Publisher will be responsible for ensuring compliance with any additional obligations, such as enhanced notice and consent or specific contractual terms, required for the processing of such data. Notwithstanding anything to the contrary, to the extent permitted by Data Protection Law, Agency may use and retain any deidentified or aggregate consumer information related to the Services for any purpose in accordance with Data Protection Law, including but not limited to developing analytics and improving the Services.

3. Security. Agency shall implement and maintain security procedures and practices appropriate to the nature of the Personal Data designed to protect the Personal Data from a Security Incident. The minimum technical and organizational measures to be implemented by Agency are set forth in Schedule 2. Agency shall regularly monitor compliance with these measures, and shall not materially decrease the overall security of the Services with respect to Personal Data during its provision of the Services. Agency shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.

4. Security Incidents. Agency shall notify Publisher without undue delay after becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in possession or control of Agency (a "**Security Incident**"). Agency shall make reasonable efforts to identify the cause of such Security Incident and take steps as Agency deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within Agency's reasonable control and required by law.

5. Subprocessors. Publisher provides general written authorization for the use by Agency of the Subprocessors identified in Schedule 3. Agency will enter into a written agreement with each Subprocessor containing data protection obligations no less protective than those in this DPA with respect to the protection of Personal Data. Agency shall notify Publisher in writing of any new Subprocessor before authorizing that new Subprocessor to process Personal Data, and Publisher may object to the new Subprocessor within ten (10) days of Publisher's receipt of notice. In the event Publisher objects to the new Subprocessor, Agency will use commercially reasonable efforts to make available to Publisher a change in the Services to avoid processing of Personal Data by the objected-to new Subprocessor. If Agency is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Publisher may terminate the applicable Services which cannot be provided by Agency without the use of the objected-to new Subprocessor by providing written notice to Agency. Agency shall be liable for the acts and omissions of its Subprocessors to the same extent Agency would be liable if performing the services of each Subprocessor directly under the terms of this DPA.

6. Vendors. Publisher authorizes Agency to engage Vendors in connection with the Services. For the avoidance of doubt, a Vendor is not a Subprocessor but rather a separate processor or controller engaged at the direction and for the benefit of Publisher. As between the parties, Publisher is solely responsible for the legality under Data Protection Law for the use of any Vendor. Agency is not intended to be a liability intermediary. Publisher agrees that certain parts of the Services may require the use of a

specific Vendors and if Publisher denies use of such Vendor, Publisher may not be able to receive Services associated with that Vendor. In some instances, a Vendor may require Agency to impose certain additional written terms on Publisher, and, in such instances, Publisher agrees to comply with such written terms.

7. Requests and Assistance. To the extent legally permitted, Agency shall: (a) promptly notify Publisher if Agency receives a request from a Data Subject to exercise their rights under Data Protection Law or receives a request or complaint from a supervisory authority, regulator, or other third party (“Request”); and (b) not respond to the Request without written approval from Publisher. Taking into account the nature of the processing, Agency shall reasonably assist Publisher in the fulfilment of Publisher’s obligation to respond to the Request. Upon request by Publisher, Agency shall reasonably assist Publisher as necessary to carry out data protection impact assessments related to Publisher’s use of the Services, and in the cooperation or prior consultation with supervisory authorities or regulators in the performance of Agency’s tasks relating to the data protection impact assessments. To the extent legally permitted, Publisher shall be responsible for any costs arising from Agency’s provision of assistance hereunder. Publisher acknowledges that Agency may not be able to fulfill Requests where doing so would interfere with Agency’s ability to comply with applicable law or legal obligation, or protect its rights or those of a third party. Each party shall provide reasonable assistance to the other party as necessary for the other party to fulfill its obligations under Data Protection Law.

8. Return and Deletion. Agency shall return or delete (at Publisher’s discretion) all Personal Data when such Personal Data is no longer needed to perform the Services, or sixty (60) days following termination of the Agreement upon Publisher’s request. Agency may retain Personal Data where necessary for Publisher to comply with applicable law or legal obligation, or protect its rights or those of a third party.

9. Audit. Agency shall allow for and contribute to reasonable audits conducted by Publisher or a third party auditor designated by Publisher to ascertain Agency’s compliance with this DPA to the extent required by Data Protection Law, provided that such audits shall be conducted upon request of Publisher at reasonable intervals (no greater than once per year), be limited to any Agency facilities where it processes Personal Data, require at least thirty (30) days prior notice, take place during normal business hours, and not require Agency to provide access to systems or information relating to its other customers. Any third party auditor must be agreed upon by Agency (not to be unreasonably withheld) and submit to a duty of confidentiality with respect to the audit. As an alternative to the foregoing, to the extent permitted by Data Protection Law, at least annually Agency may arrange for a qualified and independent third party to conduct a comprehensive audit of Agency’s policies and technical and organizational measures in support of its obligations under this DPA using an appropriate and accepted control standard or framework and audit procedure for such audits, and provide the results of such audit to Publisher upon request of Publisher. To the extent permitted by Data Protection Law, Publisher is responsible for and shall reimburse Agency for any expenses associated with this Section 9. Any information associated with this audit right shall be Agency’s confidential information and subject to obligations of confidentiality. The parties agree that, to the extent permitted by Data Protection Law, any audits described in the Standard Contractual Clauses shall be carried out in accordance with this Section 9.

10. Data Transfer. Publisher acknowledges that Personal Data will be stored and processed in the United States and other countries in which Agency or its Subprocessors maintain facilities. By using the Services, Publisher agrees to the transfer of Personal Data outside of the country in which it was provided. For any transfers of Personal Data subject to GDPR to countries (or territories or sectors within a country) or international organizations which do not benefit from an adequacy decision under GDPR, the parties hereby agree to transfer the Personal Data pursuant to the standard contractual clauses set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard

contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)) (“**Standard Contractual Clauses**”), which are incorporated herein as follows:

- a. Module Two will apply.
- b. In Clause 7 (Docking clause), the optional docking clause will apply.
- c. In Clause 9 (Use of sub-processors), Option 2 will apply and the time period for prior notice of Subprocessor change shall be set out in Section 5 of this DPA.
- d. In Clause 11 (Redress), the optional language shall not apply.
- e. In Clause 17 (Governing Law), Option 1 will apply, and the member state will Ireland.
- f. In Clause 18 (Choice of Forum and Jurisdiction), the member state will Ireland
- g. Annex I is completed as follows:
  - 1. List of Parties: Publisher is the data exporter and Agency is the data importer. The address, contact details and activities relevant to the transfer for the data exporter and data importer are set out in the Agreement and this DPA. By signing this DPA, the data exporter and data importer will be deemed to have signed Annex I.
  - 2. Description of Transfer: The required information is set out in Schedule 1.
  - 3. Competent Supervisory Authority: The data exporter’s competent supervisory authority will be determined in accordance with GDPR.
- h. Annex II is completed as follows: The required information is set out in Schedule 2.
- i. Annex III is completed as follows: The required information is set out in Schedule 3.

For any transfers of Personal Data subject to UK GDPR to countries (or territories or sectors within a country) or international organizations which do not benefit from an adequacy decision under UK GDPR, the parties hereby agree to transfer the Personal Data pursuant to the same Standard Contractual Clauses, subject to the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf> (“**UK Addendum**”). With respect to the UK Addendum, Table 1 is completed using the information set out in “List of Parties” above. Table 2 is completed using the version of the Standard Contractual Clauses listed above. Table 3 is completed using the information set out in “List of Parties” and “Description of “Transfer” above, and in Schedule 2 and Schedule 3. Table 4 is completed so that either the data importer or data exporter may end the UK Addendum when the approved Addendum changes.

11. Liability. To the maximum extent permitted by applicable law, and notwithstanding anything to the contrary, each party’s liability under this DPA is subject to the disclaimers and limitations of liability in the Agreement.

## **Schedule 1 to Data Processing Addendum**

### **Details of Processing Activities**

- **Subject Matter:** The subject matter of the processing is Personal Data.
- **Duration:** The duration of the processing is until the earlier of (i) request by Publisher to stop further processing; (ii) expiration/termination of the DPA; or (iii) when processing is no longer necessary for purposes of Agency performing its obligations pursuant to the DPA.
- **Categories of Data Subjects:** The categories of Data Subjects whose Personal Data is processed include: (i) end users of Publisher; (ii) personnel and agents of Publisher; (iii) personnel and agents of Publisher's customers, business partners, and vendors; and (iv) any other natural persons authorized by Publisher.
- **Categories of Personal Data:** The categories of Personal Data processed include:
  - **Identifiers:** IP address, cookie IDs, device advertising identifiers (e.g., IFA/IDFA, AAID), and other similar online or persistent identifiers.
  - **Internet or Other Electronic Network Activity Information:** Information regarding an end-user's interaction with an internet website, application, or advertisement, including, but not limited to, ad requests, ad impressions, clicks, and video ad metrics (e.g., start, quartiles, completion).
  - **Geolocation Data:** Non-precise location information derived from IP address.
  - **Inferences:** Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, or behavior for the purpose of serving targeted advertising.
- **Frequency of Transfers:** The frequency of the transfer of Personal Data from Publisher to Agency will be on a continuous basis.
- **Nature of Processing:** The nature of the processing is the Services as described in the Agreement.
- **Purpose:** The purpose of the processing is for Agency to provide the Services to Publisher as set out in the Agreement.
- **Business Purpose:** The business purpose as defined by CCPA is performing services on behalf of Publisher, including analytic services, storage services, advertising and marketing services except for cross-context behavioral advertising, and other similar services.
- **Location:** The Services are intended to cover the United States.
- **Retention:** Agency may retain Personal Data through the duration as described above, and after the duration where applicable law requires retention of the Personal Data, and subject to the obligations in the DPA.
- **Sensitive Data:** The Services do not involve the processing of sensitive Personal Data.
- **Subprocessors:** Any transfer of Personal Data from Agency to Subprocessors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Subprocessors are as described above.

## **Schedule 2 to Data Processing Addendum**

### **Technical and Organizational Measures to Ensure the Security of Personal Data**

This Schedule 2 describes the technical and organizational measures implemented by Agency to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

#### **Minimum Technical and Organization Measures**

A. Agency shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Schedule 2.

B. More specifically, Agency's security program shall include, at a minimum:

#### **Access Control of Processing Areas**

Agency shall implement and maintain appropriate measures to prevent unauthorized access to the data processing equipment (namely telephones, database and application servers and related hardware) where Personal Data is processed or used, including:

- establishing security areas and physical controls;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- access to the data center where Personal Data is hosted is logged, monitored, and tracked; and
- the data center where Personal Data is hosted is secured by a security alarm system, and other appropriate security measures.

#### **Access Control to Data Processing Systems**

Agency shall implement and maintain appropriate measures to prevent data processing systems where Personal Data is processed and used from being used by unauthorized persons, including:

- use of industry standard encryption technologies;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- access to data content is logged, monitored, and tracked.

#### **Access Control to Use Specific Areas of Data Processing Systems**

Agency shall implement and maintain appropriate measures to help ensure that the persons entitled to use data processing system where Personal Data is processed and used are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of industry standard encryption technologies; and
- control of files, controlled and documented destruction of data.

### **Availability Control**

Agency shall implement and maintain appropriate measures to ensure that Personal Data is protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

### **Transmission Control**

Agency shall implement and maintain appropriate measures to help prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of industry standard firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- providing user alert upon incomplete transfer of data (end to end check); and
- data transmissions are logged, monitored and tracked.

### **Input Control**

Agency shall implement and maintain appropriate input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within Agency's organization of the input authorization; and
- electronic recording of entries.

### **Separation of Processing for different Purposes**

Agency shall implement and maintain appropriate measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within Agency's data base separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, or function they support; and

- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

### **Documentation**

Agency will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Agency will ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Schedule 2.

### **Monitoring**

Agency shall implement and maintain appropriate measures to monitor access restrictions to Agency's system administrators and to help ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of measures to register system administrators' access logs to the infrastructure and keep them secure;
- audits of system administrators' activity to assess compliance with assigned tasks and applicable laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

### **Limits on Retention/Destruction**

- Agency shall implement and maintain appropriate measures to securely destroy Personal Data. Methods of performing these actions may include the use of a third party disk scrubbing utility or destruction of the drive, such as by degaussing, shredding, or other means of physically destroying data through specialized equipment and services.

**Schedule 3 to Data Processing Addendum**

**List of Subprocessors**

Publisher has authorized Agency's use of the following Subprocessors for the processing of Personal Data:

[Name]

Address

Contact person's name, position and contact details

Description of processing]