# DATA PROTECTION TERMS

The following data protection terms and conditions (the "**Data Protection Terms**") form an integral part of the standard terms and conditions (available at https://integralads.com/terms-and-conditions/ the "**Standard Terms**") or, if applicable, the master services agreement ("**MSA**") as between Customer and Integral Ad Science, Inc. ("**IAS**") for Customer's use of IAS products and services (the "**Services**") described in the Standard Terms, MSA or an Order Form. These Data Protection Terms govern the responsibilities of the parties with respect to the processing of personal data which is subject to European Data Protection Laws (as defined below) and is processed in the course of Customer's use of the Services. All undefined capitalized Terms herein shall have the same meaning as the Standard Terms or MSA, as applicable.

In the event of any conflict or inconsistency between the Standard Terms, MSA and these Data Protection Terms, these Data Protection Terms shall govern.

The most recent version of these Data Protection Terms is available at https://integralads.com/legal-portal/eu-data-protection-terms/.

1. **Definitions**. In these Data Protection Terms:

(a) the terms "**controller**", "**processor**", "**data subject**", "**personal data**", "**personal data breach**", "**processing**" and "**supervisory authority**" have the meaning given to them in The General Data Protection Regulation (Regulation (EU) 2016/679, the "**GDPR**");

(b) the term "**European Data Protection Law**" means the GDPR and any applicable national implementations of the GDPR in Member States of the European Economic Area ("**EEA**"), any privacy and data protection laws applicable to personal data relating to individuals located in Switzerland, and, in the event that the UK leaves the EEA, the UK Data Protection Act 2018 (each as amended, superseded or replaced);

(c) the term "**Ad Performance Data**" means pseudonymous identifiers (i.e., IP addresses); and other data relating to a particular device used to navigate the internet, including non-precise location information (derived from IP address intelligence), activity related to digital advertising displayed on the device, and details related to the website or mobile app where the digital advertising was displayed. Ad Performance Data does not contain any names, phone numbers, e-mail addresses, persistent device identifiers or other contact details;

(d) the "**C-to-C Transfer Clauses**" means the Standard Contractual Clauses for Controller-to-Controller Transfers set out at https://integralads.com/legal-portal/eu-controller-to-controller-standard-contractual-clauses/;

(e) the "**C-to-P Transfer Clauses**" means the Standard Contractual Clauses (for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection) set out at https://integralads.com/legal-portal/eu-controller-to-processor-standard-contractual-clauses/;

(f) "**Emergency Replacement**" means the sudden replacement of a sub-processor where such change is outside of IAS's reasonable control (such as if the sub-processor ceases business, abruptly discontinues services to IAS, or breaches its contractual duties owed to IAS);

(g) "**sub-processor**" means a third party data processor engaged by IAS in its capacity as a processor which has (or potentially will have) access to or processes personal data for and on behalf of Customer;

(h) "**IAS Technology**" means pixels, ad tags and/or software development kits (SDKs) utilized in the provision of Services to Customer.

(i) terms which are defined in the Standard Terms shall have the same meanings in these Data Protection Terms as are set out in the Standard Terms or MSA, as applicable.

2. **Applicability of these Data Protection Terms**. These Data Protection Terms apply only when, and to the extent that, Customer or IAS processes personal data which is subject to European Data Protection Law in the course of providing or receiving the Services or in the course of performing or exercising its rights and obligations under the Standard Terms or MSA, as applicable. The parties acknowledge that Customer is a controller of such personal data processed by IAS in the course of performing or exercising its rights or obligations under the Standard Terms or MSA, as applicable. Customer further acknowledges that IAS acts as a controller for the processing described in Schedule 1 to these Data Protection Terms, and as a processor for the processing described in Schedule 2 to these Data Protection Terms.

3. **Obligations where IAS acts as either a controller or a processor**. Irrespective of whether IAS acts as a controller or a processor, Customer shall:

(a) ensure that all necessary consents (if any) are obtained and all necessary notices and/or consent withdrawal mechanisms (if any) are provided (whether by applicable publishers, industry initiatives, Customer or otherwise) so as to enable IAS to obtain and process lawfully in accordance with European Data Protection Law(s) the information IAS collects and processes in providing the Services (Schedules 1 and 2); and

(b) ensure that all advertising content containing IAS Technology displays a link from which Customer's privacy notice is accessible, and shall ensure that its privacy notice describes the processing set out in Schedules 1 and 2, including the transfer of personal data to IAS, in a manner which complies with European Data Protection Laws. IAS will provide Customer with such information as the Customer may reasonably request in order to comply with this obligation.

Further, each party shall:

(a) comply with its obligations under European Data Protection Laws, and shall not take any action or make any omission which might be reasonably likely to put the other party in breach of European Data Protection Laws;

(b) put in place appropriate industry-standard technical and organizational measures to ensure a level of security for personal data appropriate to the risks of the processing, including unauthorized or unlawful processing and against accidental loss, destruction or damage, and in particular IAS shall put in place at least the measures set out at https://integralads.com/ias-data-protection-portal/ias-technical-and-organizational-security-measures/;

(c) notify the other party without undue delay after becoming aware of a personal data breach affecting personal data processed in the course of performing or exercising its rights and obligations under the Standard Terms or MSA, as applicable, in which case the party that has suffered the personal data breach shall provide reasonable assistance to the other in relation to remediating the personal data breach and complying with related obligations under European Data Protection Law;

(d) provide reasonable assistance to the other in the event of any complaint, request or communication from a supervisory authority or data subject alleging non-compliance with European Data Protection Laws as a result of the processing carried out under this Agreement;

(e) provide reasonable assistance requested by the other in relation to compliance with any obligations under European Data Protection Laws, including providing any additional disclosures and enabling any additional data subject controls that the parties agree are necessary pursuant to European

Data Protection Laws for the setting of IAS Technology and/or the processing or collection of Ad Performance Data (via the IAS Technology or otherwise), neither party will unreasonably withhold or delay its agreement to any proposal in this regard.

4. **Obligations where IAS acts as a controller**. In relation to the processing described in Schedule 1 by IAS, where it acts as a controller:

(a) Customer will provide IAS with such information and co-operation as IAS may reasonably request to assist IAS in complying (and evidencing its compliance) with European Data Protection Law(s) in relation to the provision of information about IAS's processing to data subjects;

(b) If IAS uses the Ad Performance Data to create black lists as described in Schedule 1, IAS shall use all reasonable endeavours to keeps such blacklists up to date and accurate; and

(c) each party shall provide reasonable assistance to the other on request in relation to any requests the other party receives from individuals in relation to exercising their rights under European Data Protection Laws.

5. **Obligations on IAS where IAS acts as a processor**. Where IAS acts as a processor (as described in Schedule 2), IAS warrants that it shall:

(a) process personal data only on Customer's instructions, as documented in Schedule 2 to these Data Protection Terms or as otherwise required by applicable law;

(b) ensure that all individuals authorized to process personal data are subject to an obligation to keep that personal data confidential;

(c) provide Customer with reasonable assistance in relation to Customer's obligations under European Data Protection Laws, including in relation to responding to requests from individuals to exercise their rights, carrying out data protection impact assessments and consulting with supervisory authorities where required by law;

(d) with respect to sub-processors:

(i) with the exception of Emergency Replacements, only engage further sub-processors where such engagement is notified to Customer prior to such engagement commencing by way of updating the list of sub-processors at https://integralads.com/legal-portal/ias-list-of-subprocessors/, which Customer may subscribe to receiving updates to thereby giving Customer an opportunity to object to such engagement. Customer may elect to opt-in to receive updates to IAS's list of sub-processors here;

(ii) If Customer objects to any such changes to the list of sub-processors on reasonable grounds relating to the protection of personal data, Customer can do so within fifteen (15) calendar days of receiving such an update by following the instructions set out in such update;

(iii) If Customer does not object during such time-period, the new sub-processor(s) shall be deemed to be agreed and consented to by Customer, also according to Clauses 5(h) and 11 of the C-to-P Transfer Clauses; and

(iv) In the event of such an objection, the parties shall discuss the objection in good faith and shall take reasonable steps to find a mutually agreeable remedy to Customer's objection, by one of the following options: (1) IAS will abort its plans to use the sub-processor with regard to Customer's personal data; or (2) IAS will take the corrective steps requested by Customer in its objection (which remove customer's objection) and proceed to use the sub-

processor with regard to Customer's personal data; or (3) IAS may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the service that would involve use of the sub-processor with regard to Customer's personal data. If no such remedy can be found within ninety (90) calendar days after the objection has arisen, either party shall have the right to terminate any Services provided to Customer by IAS which would involve the processing of personal data by the objectionable sub-processor.

(v) Where an Emergency Replacement is required, IAS will inform Customer of the Emergency Replacement as soon as possible and the process to formally appoint such sub-processor defined above shall be triggered.

(vi) All processing by such further sub-processors is subject to an agreement with further sub-processors which contains all the terms required by European Data Protection Laws, and where IAS remains fully liable to Customer for the performance of the further sub-processor's obligations;

(e) make available all information reasonably requested by Customer in relation to its processing of personal data;

f) allow for and contribute to audits, including inspections, where required by Customer to comply with legal obligations to which Customer are subject. Customer shall take all reasonable steps to give IAS reasonable prior notice of any such audits, and shall be responsible for all reasonable costs incurred by IAS in participating in such an audit, calculated on a time and materials basis and

(g) upon Customer's written request, return to Customer or delete all personal data processed at the termination of the processing described in Schedule 2 or otherwise deleted in accordance with IAS's standard data retention policies.

**6. International Data Transfers**. Customer acknowledges that personal data is processed by IAS, which is located in a country outside the EEA which is not considered to provide an adequate level of protection for personal data. In order to ensure such transfers of personal data are lawful, the parties hereby enter into the C-to-C Transfer to the extent that IAS acts as a controller (as described in Schedule 1) and the C-to-P Transfer Clauses to the extent that IAS acts as a processor (as described in Schedule 2). Agreement to these Data Protection Terms shall be considered as signature to the C-to-C Transfer Clauses and the C-to-P Transfer Clauses, which shall take effect from the date of Customer's acceptance of the Standard Terms. In the event of any conflict between the Standard Terms, MSA, these Data Protection Terms, the applicable Order Form or SOW and the C-to-C Transfer Clauses or the C-to-P Transfer Clauses, then in order of precedence, the C-to-C Transfer Clauses or C-to-P Transfer Clauses (as applicable) shall prevail, then these Data Protection Terms, MSA, Standard Terms, Order Form or SOW, as applicable.

Dated October 18, 2019

**Schedule 1**
**PROCESSING BY IAS AS A CONTROLLER**

**Categories of Data Subjects:**

- Visitors to websites/mobile applications owned and operated by Customer
- Users of the Services on which Customer's advertising is displayed

**Purposes of processing:**

- **Ad Fraud processing --** algorithmic modeling and heuristics to detect non-human (bot) fraudulent activity in the ad stream. IP addresses are extracted from X-Forwarded-For HTTP header field of HTTP requests sent to IAS's network firewall servers through IAS Technology. The IAS ad fraud team will run through iterations of behavioral and network analysis fraud models where IP addresses shown to be generating fraudulent traffic are added to Fraud IP Blacklist. Fraud IP Blacklist is utilized to block ads from serving to users reporting from the IP addresses on IAS's Fraud IP Blacklist;
- Anonymization of Ad Performance Data, in accordance with European Data Protection Laws, for use for other purposes.

**Categories of Personal Data:**

- Ad Performance Data

**Recipients of Personal Data:**

- Subcontractors and other service providers to IAS; Customers of IAS who contract for its ad fraud/botnet identifier solutions.

**Retention information**

- IAS shall retain the Ad Performance Data for no longer than thirteen (13) months and IAS shall retain IP addresses within its Ad Performance Data for no longer than thirty (30) days.

## Schedule 2
## PROCESSING BY IAS AS A PROCESSOR

**Subject-matter of the processing:**

- The subject matter of the processing carried out by IAS as a processor is the performance of certain services on Customer's behalf.

**Duration of the processing:**

- The duration of the processing shall be the duration of the Services performed by IAS.

**Nature and purpose of the processing:**

In order to provide the services, IAS is given access to data relating to data subjects' online behaviors, including the IP address associated that is reported as being associated with such data subject. IAS uses such data to provide the services and reporting to Customer, including:

- **Brand safety processing –** assigning IAS brand safety taxonomy to an ad placement in a browser or app;
- **Viewability processing --** measuring ad viewability in a browser or app; and
- **Geo-compliance processing –** verifying location of user where ad is served using non-precise location data associated with IP address.

**Categories of Personal Data:**

- Ad Performance Data
- Customer has no access to raw Ad Performance Data as it is transferred directly to IAS via IAS Technology

**Categories of Data Subjects:**

- Visitors to websites owned and operated by Customer
- Users of the Services on which Customer's advertising is displayed

**Retention information**

- IAS shall retain the Ad Performance Data for no longer than thirteen (13) months and IAS shall retain IP addresses within its Ad Performance Data for no longer than thirty (30) days.

**Security measures in place:**

- The technical and organizational measures are available at https://integralads.com/ias-data-protection-portal/ias-technical-and-organizational-security-measures/.