Institute for Advertising Ethics
Policy 1: Basic GDPR Data Protection Policy

This policy addresses the foundational principles of the GDPR; most particularly, Articles 1-10, 36 and 58.

Last updated	11/1/2022

Definitions

COMPANY	means the Institute for Advertising Ethics, a registered 501c3.
GDPR	means the General Data Protection Regulation.
RESPONSIBLE PERSON	means Andrew Susman, COO
Register of Documents	means a register of all documents kept by the COMPANY to show compliance with the provisions of Data Privacy legislation.

1. DATA PROTECTION PRINCIPLES

The COMPANY is committed to the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and to the processing of data in accordance with the COMPANY'S responsibilities under the principles articulated in Articles 5-10 and 58 of the GDPR. The COMPANY acknowledges and adopts the subject matter, objectives, material scope and territorial scope of the GDPR as articulated in Articles 1-3.

The COMPANY adopts the definitions contained in Article 4 of the GDPR, and in particular that "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Accordingly, the COMPANY requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

2. GENERAL PROVISIONS

a. This policy applies to all personal data processed or controlled by the COMPANY.

b. The RESPONSIBLE PERSON shall take responsibility for the COMPANY's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

d. The COMPANY may have registered, or be required to register, with a Supervisory Authority, or pay fees, as an organization that controls and processes personal data under its supervision. A copy of the registration and related materials shall be held in the Register of Documents.

e. The COMPANY may have designated, or be required to designate, a representative in the European Union. A copy of the designation and related materials shall be held in the Register of Documents.

f. The COMPANY shall comply with an order, or a temporary or definitive limitation, on processing or the suspension of data flows, by the Supervisory Authority

g. The COMPANY shall provide lawful access to the Supervisory Authority.

3. LAWFUL, FAIR AND TRANSPARENT PROCESSING

a. To ensure its processing of data is lawful, fair and transparent, the COMPANY shall maintain a Register of Documents, which shall include a list of systems, co-controllers, processors and sub-processors as well as associated documentation. The Register of Documents shall be reviewed at least annually.

b. Individuals have the right to access their personal data and any such requests made to the COMPANY shall be dealt with in a timely manner.

c. All co-controllers, processors and sub-processors shall agree to follow these principles and this POLICY or one substantially similar as well. Copies of such agreements shall be maintained in the Register of Documents.

d. The COMPANY shall follow Article 5 of the GDPR, and assure that (i) all processing is lawful, fair and transparent, (ii) collection is for a specific, explicit and legitimate

purpose, (iii) processing is adequate, relevant and limited, (iv) data is accurate and updated, (v) data is kept only for as long as necessary and (vi) data is processed with adequate security.

4. LAWFUL PURPOSES

a. All data processed by the COMPANY or for the COMPANY must be done on one of the lawful bases contained in Article 6 of the GDPR: consent for specific purpose, performance of contract, legal obligation of the controller, vital interests of the data subject or a natural person, task in the public interest or legitimate interest (unless overridden by interests or rights of the data subject). The COMPANY, shall note the appropriate lawful basis in the Register of Documents.

b. The COMPANY, where relying upon consent shall not condition the provision of service upon consent (unless required), such consent shall be of genuine free choice and may be withdrawn without detriment.

c. The COMPANY, where Controller and relying upon consent as the lawful basis for processing, shall be able to demonstrate consent by the data subjects by a clear affirmative act, informed and based upon a request that is clearly distinguishable from other matters, intelligible and easy to read. Documentation sufficient to demonstrate consent shall be kept in the Register of Documents.

d. The COMPANY, where controller, to demonstrate and ensure processing is in accordance with the principles of the GDPR, shall file proof of appropriate technical and organizational measures in the Register of Documents.

e. The COMPANY, where controller, to demonstrate processing by design and by default under Article 25 of the GDPR, will file appropriate documentation in the Register of Documents.

f. Where consent is relied upon as a lawful basis for processing data, the request for consent shall be in a clearly presented and distinguishable manner, and evidence of opt-in consent shall be kept with the personal data.

g. The option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the COMPANY's systems.

h. Special consideration to Article 8 of the GDPR shall be given concerning a child's consent.

i. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited absent a special condition identified in Article 9 of the GDPR. Where there is an applicable exception, it must be documented.

j. Processing of personal information relating to criminal convictions and offenses or related security measures is prohibited absent special conditions identified in Article 10 of the GDPR.

5. DATA MINIMIZATION

The COMPANY shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. ACCURACY

a. The COMPANY shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. ARCHIVING / REMOVAL

a. To ensure that personal data is kept for no longer than necessary, the COMPANY shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

c. The GDPR imposes record keeping obligations upon the COMPANY. Such records, as required by the GDPR and the COMPANY's policies shall be kept in the Register of Documents.

8. SECURITY

a. The COMPANY shall ensure that personal data is stored securely using systems that are kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

e. The COMPANY shall maintain proof of appropriate security, as required under Articles 5 and 32 in the Register of Documents.

9. BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the COMPANY shall promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the relevant government authority and the data subjects affected.

10. PRIOR CONSULTATION

Where a data-protection impact assessment indicates that processing operations involve a high risk (which the controller can or cannot mitigate by appropriate measures in terms of available technology and costs of implementation), a consultation with the supervisory authority shall take place prior to the processing. The COMPANY shall comply with the provisions of Article 36 in such event, including supplying the supervisory authority with the applicable and required information.

END OF POLICY