Checklist for Self-Attesting Digital Advertising Assurance Providers

Instructions for Completing the Checklist

Companies who self-attest compliance with the TAG "Core Criteria for Effective Digital Advertising Assurance" should adhere to the following enumerated items for one or more of the Core Criteria for which they are seeking to be recognized. In addition, companies should adhere to the Key Performance Indicators as periodically determined and set forth by TAG.

Entities that wish to receive a TAG "Certified Against Piracy" Seal as a Self-Attesting DAAP should submit to TAG a completed Self-Attestation Checklist and supporting materials for the Core Criteria for which the Self-Attesting DAAP is seeking to be recognized.

Criteria-Specific Attestations

A Self-Attesting Entity should submit to TAG the Criteria-Specific Attestations set forth below with supporting documentation or materials for one or more of the Core Criteria for which they are seeking to be recognized. Effective utilization of services of a Validated DAAP may serve as evidence of adherence to the Core Criteria. Supporting documentation provided by Self-Attesting Entities and their agents as part of the self-attestation process shall be treated as confidential by TAG, unless otherwise noted.

Criterion #1: Identify Ad Risk Entities ("AREs").

1. Company should assess whether entities are AREs. *Please provide examples or reports of the effectiveness of this technology.*

2. Company should provide tools to help advertisers and/or their agencies decide the extent to which they wish to limit or restrict the display of their advertisements on entities deemed to be AREs in Core Criteria section (IV)(1)(a). *Please provide examples.*

3. Company should have an objective review and evaluation process for claims from entities of erroneous designation or scoring or determination of those entities as AREs in Core Criteria section (IV)(1)(a). *Please provide an overview of the process.*

Criterion #2: Prevent Advertisements on Undesired AREs.

1. Company should restrict or enable the restriction of the display of advertisements on undesired AREs in accordance with the direction of an advertiser and/or its agency as set forth in Core Criteria section (IV)(1)(b) ("Undesired AREs"). *Please provide examples or reports showing the effectiveness of this technology.*

2. Company should provide or enable the provision of real-time solutions as a means to effectively prevent advertisements on Undesired AREs. *Please provide examples or reports showing the effectiveness of this technology.*

Criterion #3: Detect, Prevent, or Disrupt Fraudulent or Deceptive Transactions.

1. Company should have protocols and capabilities to detect, prevent, or disrupt advertising placements on Undesired AREs that are transacted fraudulently or deceptively (e.g., through the use of intermediary sites or other means to disguise the ARE's identity or purpose). *Please provide an overview of the protocols or reports of the effectiveness of these protocols.*

2. In the event that a Company identifies the use of intermediary sites or other means as set forth in Core Criteria section (IV)(3)(a), the Company should have protocols and capabilities to prevent further advertisement exposure through such means. *Please provide an overview of the protocols or reports of the effectiveness of these protocols.*

3. Company should have an objective review and evaluation process for claims from entities of erroneous determination of fraudulent or deceptive transactions in Core Criteria section (IV)(5)(a). *Please provide an overview of the process.*

Criterion #4: Monitor and Assess for Advertisement Placement Compliance.

1. Company should detect and report on advertisements on AREs that may not be in compliance with advertiser/agency instructions, thus enabling advertisers and agencies to implement remedial action. *Please provide examples of such reports and an overview of the detection process.*

Criterion #5: Eliminate Payments to Undesired AREs.

1. Company should have technology and protocols in place that prevent or enable the prevention of payments resulting from advertisements displayed on Undesired AREs. *Please provide an overview of the protocols and examples of the technology in practice or reports of the effectiveness of this technology.*

2. In the event payment has been made to Undesired AREs, Company should have technology and protocols in place that enable the reversal or reclamation of such payment. *Please provide an overview of the protocols and examples of the technology in practice or reports of the effectiveness of this technology.*

Complaint Resolution Procedures

Complaints should be submitted directly to the Self-Attesting DAAP:

Fields to include:

a. Incident ID;
b. Copyright Holder;
c. Infringing URL;
d. Framing URL;
e. Creative URL;
f. Date found; and
g. Screenshot (optional).

A Self-Attesting DAAP should respond to complaints using a TAG provided form/format that includes:

1. Received;

2. Under investigation;

3. Actioned; or

4. Refuted:
    a. No rights violation;
    b. No usage of company's product;
    c. No usage of company's monetization products;
    d. Insufficient information for self-attested DAAP to investigate the complaint; and/or
    e. Complaint has already been actioned.

If the remediation or refutation of the complaint is not accepted by the complainant, the complainant may forward the complaint to TAG for elevation to a Formal Compliance Review.

Formal Compliance Review

Discovery & Initial Evaluation of Potential Non-Compliance Information

1. TAG shall accept and evaluate notices and referrals from rights holders, advertisers, and others as determined by TAG that purport to provide credible evidence of a pattern or practice of non-compliance by an Self-Attesting DAAP.

2. TAG should review credible information about potential non-compliance of Self-Attesting DAAP. Part of this review shall involve engagement with the Self-Attesting DAAP in question. An initial finding of (i) a pattern or practice of knowingly delivering ads to AREs, or (ii) a lack of due diligence to discover or fix gaps in detection of AREs, shall result in a formal review of the company's standing in the TAG "Certified Against Piracy" Seal program. However, occasional, isolated instances of Self-Attesting DAAPs placing digital ads on sites associated with an undesired risk of infringement shall not, in and of itself, constitute grounds to institute a review of the entity's standing in the TAG "Certified Against Piracy" Seal program.

Formal Review Procedures

1. Once a formal review of a Self-Attesting DAAP has commenced, TAG shall work with the Self-Attesting DAAP to determine the source of potential non-compliance. TAG shall disclose the substance of the credible information leading to the Formal Compliance Review, and, unless there is a demonstrated need for confidentiality, shall share the source of that information in order to facilitate the Self-Attesting DAAP's internal investigation.

2. If the review determines that the Self-Attesting DAAP does not consistently adhere to the Core Criteria, the Self-Attesting DAAP should be deemed to be in non-compliance. Anecdotal evidence, cases of temporary technical glitches, criminal actions committed against the Self-Attesting DAAP shall not without additional factors be determined to constitute non-compliance by the Self-Attesting DAAP. Such factors may be considered in the overall Formal Compliance Review process.

3. Information obtained through the Formal Compliance Review process from Self-Attesting DAAPs and their agents shall be treated as confidential by TAG.

Review of TAG "Certified Against Piracy" Seal Qualifications

1. Upon a determination that a Self-Attesting DAAP is in non-compliance, the Self-Attesting DAAP shall have 30 days to show that the entity has taken remediation steps and is now in compliance with the self-attestation process.

2. Within 30 days of receiving information regarding the remediation steps taken and/or that the complaint was in error, TAG shall provide a written decision explaining its decision and reasoning.

3. If a Self-Attested DAAP is found to be in non-compliance more than once within any 2-year time frame, that company forfeits their current TAG "Certified Against Piracy" Seal and should complete the full Validation process in order to receive a future TAG "Certified Against Piracy" Seal.

Key Performance Indicators

The TAG Self-Attestation Working Group will determine thresholds for Key Performance Indicators (KPIs) that will constitute the thresholds that Self-Attesting DAAPs should meet in order to avoid further disclosures and review by TAG or a validator. KPIs and the associated thresholds will be released as a separate document that is expected to be revised regularly to reflect marketplace changes. Recommended KPIs:

A. Average time elapsed to acknowledge a complaint;

B. Average time elapsed to remediate the problem asserted in the complaint;

C. Rate of successful remediation of acknowledged complaints; and

Assessments of noncompliance at any level, including what constitutes "credible evidence of a pattern or practice of non-compliance by a Self-Attested DAAP," will be made based on the Key Performance Indicators, which will be periodically updated by the TAG Self-Attestation Working Group.

Still Have Questions?

Learn more at www.tagtoday.net, or reach out to TAG with your questions at info@tagtoday.net.