Self-certification Criteria for companies participating in the European Self-Regulatory Programme on OBA

Document version: 1.1

Date: 16 November 2012

1. Introduction

The European Interactive Digital Advertising Alliance ('EDAA') is a non-profit organisation based in Brussels and is responsible for enacting key aspects of the self-regulatory initiative for Online Behavioural Advertising ('OBA') across Europe. EDAA principally acts as the central licensing body for the OBA Icon and provides technical means for consumers to exercise transparency and control over OBA through the online consumer choice platform at www.youronlinechoices.eu. EDAA is governed by EU-level organisations which make up the value chain of OBA within Europe and acts to ensure European (and global) consistency in approach.

The Self-Regulatory Initiative on OBA is based on the European Industry Self-Regulatory Framework on Data Driven Advertising, aimed to increase transparency and control for Online Behavioural Advertising, and being an integral part of the European Advertising Standards Alliance's ('EASA') comprehensive self-regulatory Best Practice Recommendation ('BPR') for Online Behavioural Advertising; together, these documents outline the Principles of the European Programme for OBA.

Under Principle VI – Compliance and Enforcement Programmes, the European Industry Self-Regulatory Framework on Data Driven Advertising states that:

"*Following the adoption of this Framework and the Icon each Company should comply and self certify by 30 June 2012. Companies adopting the Framework later than 1 January 2012 should comply and self certify within 6 months of adopting the Framework and the Icon.*"

In line with the above, this document aims to provide companies participating in the European Programme on OBA with a comprehensive set of criteria for of compliance. of compliance shall be limited to those requirements applicable to each signatory's business model; however, should a signatory be subject to multiple obligations, - must cover all such applicable provisions. In other words, if a signatory fulfils more than one role in the advertising ecoi system, then it should comply with the requirements applicable to each of these roles.

of compliance under this document and the European Principles Documents does not exempt Companies from fulfilling their obligations under applicable national laws.

This document is based on the *European Industry Self-Regulatory Framework on Data Driven Advertising*, *EASA Best Practice Recommendation on Online Behavioural Advertising* and the *Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe*.

2. Criteria for self-certification of compliance – Third Parties

Under the terms of the *European Principles Documents*, a number of provisions apply to signatory companies acting as Third Parties.

In practice, a signatory company may simultaneously play several roles; in such circumstances, self-certification must cover all applicable provisions.

For the purposes of this document, a number of roles have been identified:

- Advertisers. An Advertiser is an entity that pays for the production, execution, and placement of an online advertisement, usually for one of its own products or services.
- Agencies. An Agency is an entity that manages the production, execution, or placement of an online advertisement on behalf of the Advertiser.
- Third Parties. As defined by the European Industry Self-Regulatory Framework on Data Driven Advertising, an entity is a Third Party to the extent that it engages in Online Behavioural Advertising on a web site or web sites other than a web site or web sites it or a an entity under Common Control owns or operates. The following (but not limited to) can be examples of Third Parties:
    - Ad Networks. An Ad Network is an entity that connects Advertisers to web sites that host online advertisements, optimizing value for both Advertiser and Publisher.
    - Ad Servers. Ad Servers are entities that provide specialized software to Publishers, Advertisers and Ad Networks to deliver and report on online advertising campaigns.
    - OBA Providers. An OBA Provider is an entity that develops and uses or provides in the marketplace technology to collect data for OBA purposes and to deliver OBA Ads[1].
    - Ad Exchanges. Ad Exchanges represent technology platforms that facilitate automated auctioni based pricing and buying of online advertising inventory in reali time. Ad Exchanges represent a sales channel to Publishers and Ad Networks, and a source of online advertising inventory for Advertisers and Agencies.
    - Demand Side Platforms. A Demand Side Platform (DSP) is a system that allows Advertisers to manage their bids across multiple Ad Exchanges in order to minimize expenditure while maximizing results.
    - Supply Side Platforms. A Supply Side Platform (SSP) is a system that allows Publishers to automate the management of their inventory across multiple Ad Exchanges or Ad Networks, in order to maximize income.
- Publishers. A Publisher is the owner, controller or operator of the web site with which the web user interacts. The European Industry Self-Regulatory Framework on Data Driven Advertising refers to the Publisher as being the Web Site Operator.

[1] As defined in the *Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe*

2.1. Data security

2.1.1. Safeguards

Companies should maintain appropriate physical, electronic, and administrative safeguards to protect the data collected and used for OBA purposes, including any backups. Some examples for how this could potentially be done – but not limited to:

1. Appropriate physical safeguards. Companies may implement internal processes for ensuring OBA data security from a physical perspective. Physical access to OBA data could, even within the company, be granted only based on business reasons and all access should be monitored and logged as part of standard business practice.
2. Appropriate electronic safeguards. Companies could implement electronic data protection tools against unauthorised access, including (but not limited to) data encryption or firewalls.
3. Appropriate administrative safeguards. Companies could implement appropriate administrative measures, such as, if applicable, specific clauses in contracts with employees, partners or contractors, or any internal procedures designed to prevent unauthorised access.

2.1.2. Data Storage

Companies should retain data that is collected and used for OBA only for as long as necessary to fulfil a legitimate business need, or as required by law. Some examples for how this could potentially be done – but not limited to:

1. Set a reasonable validity interval on any data collected for OBA purposes.
2. Delete data collected for OBA purposes when the validity interval has been exceeded.

2.2. Sensitive Segmentation

2.2.1. Children's segmentation

Companies will not create segments for OBA purposes that are specifically designed to target children (age 12 and under). While this does not mean that ad delivery will cease, it means that no advertisements specifically targeted for age 12 and under will be delivered to this category.

2.2.2. Other sensitive segments

Should a Company seek to create or use such OBA segments relying on use of sensitive personal data, as defined under Article 8.1 of Directive 95/46/EC (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex-life), they must obtain a web user's Explicit Consent, prior to engaging in OBA using that information.

2.3. Education

Companies that engage in OBA should provide information to inform individuals and businesses about OBA, including easily accessible information about how data for OBA purposes is obtained, how it is used and how web user choice may be exercised.

Some examples for how this could potentially be done – but not limited to:

1. Provide information regarding their OBA business practices, either via pages on Companies' own site(s), or by linking to the OBA User Choice Site. This information should contain, at a minimum, a description of:
    a. What OBA means and how OBA works
    b. How OBA is used by the Company
    c. How data for OBA purposes is collected, stored, processed and used
    d. How user choice may be exercised
2. Information provided should be made easily accessible for users; this can be done by creating a link on the footer of the site, on the home page or on the general Terms and Conditions page, unless stated otherwise in the "Best-practice recommendations for self-certification of compliance" section below
3. Information should be provided in a language easily understood by the average Internet user (i.e. avoiding where possible technical terms and specialised wording)

2.4. Complaints handling

Web users may make complaints about incidents of suspected non-compliance with the Principles of the European Self-Regulatory Programme on OBA. While web users will have available a number of ways to make complaints, Companies must ensure that, regardless of what means the user uses to submit the complaint (whether directly to the Company or through an industry or self-regulatory body), proper processes are in place to ensure a timely and satisfactory response and resolution of the issue, if necessary.

In order to be compliant, companies should:

1. Implement and ensure efficient and timely functioning of internal complaint handling mechanisms. It is recommended that the time interval to respond to user complaints should not be more than 7 days and should address the substance of the complaint.

2. Implement an easily accessible mechanism for complaints to be filed directly with companies.

3. Ensure an efficient process in place for responding to enquiries made by national self-regulatory bodies on OBA-related issues and formal unresolved OBA complaints.

4. Adhere to the enquiring self-regulatory organisation's procedures for complaint handling[2].

2.5. Third Party Privacy Notice

Third Parties should give clear and comprehensible notice on their websites describing their OBA data collection and use practices. For the purposes of this document, 'clear and comprehensible' should be defined as simple, layman's language; also, the link to the respective notice should be easily accessible for the users (i.e. clear link on the homepage) and should be distinct from the "Terms and Conditions" section.

The notice should include the following information:

- Third party's identity and contact details;

[2] Different national self-regulatory bodies may apply slightly different complaints handling procedures; as such, should a complaint be filed-in with a self-regulatory body, the enquiry to be further made by the SRO to the company will be accompanied by the relevant set of procedures. Pan-European companies wishing to receive information in advance about the generic procedures followed by the self-regulatory bodies in Europe can address a request to the European Advertising Standards Alliance (EASA).

- The types of data collected and used for the purpose of providing OBA, including an indication as to whether any data collected is "personal data" or "sensitive personal data" as defined by the relevant national implementation of Directive 95/46/EC;
- The purpose or purposes for which OBA data is processed and the recipients or categories of recipients not under Common Control to whom such data might be disclosed;
- A link to the OBA User Choice Site;
- An easy-to-use mechanism for allowing Internet users to exercise choice with regard to the collection and use of data for OBA purposes and to the transfer of such data to Third Parties for OBA; this mechanism can be either a link to the opt-out page of the OBA User Choice Site or a more advanced User Preference Management tool implemented by the Third Party on its own web page.
- A statement to the effect that the Company adheres to these Principles:

2.6. Third Party Enhanced Notice

Third Parties should provide "enhanced notice" of the collection and use of data for OBA purposes via the Ad Marker in or around the advertisement, in accordance with the provisions of Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe.

Regardless of various arrangements with Web Site Operators or Agencies/Advertisers, the responsibility to display the enhanced notice belongs to Third Parties. For this reason, should a Third Party fail to comply with the enhanced notice obligations, it is the Third Party and not the Web Site Operator or Agency/Ad Server that will be considered to be noni compliant.

In order to display the Enhanced Notice, the Third Party must have a licence; in the European Union/European Economic Area (EU/EEA) the relevant licence can only be obtained from the European Digital Advertising Alliance, under specific terms and conditions.

2.7. User Choice

Each Third Party should make available a mechanism for web users to exercise their choice with respect to the collection and use of data for OBA purposes and the transfer of such data to Third Parties for OBA.

In practice, this means:

1. There should be a clear link from the Ad Marker or from the interstitial page[3] to the OBA User Choice Site.
2. Integration of the Third Party with the user choice mechanism hosted on the OBA User Choice Site must be in place and work reliably over time; this obligation refers mainly to OBA Providers or any Third Parties using their own means to uniquely identify a browser (i.e. cookies or any other technical solutions).
3. The practice of using technologies in order to circumvent the user's express choices (for example by deliberately "re-spawning" deleted cookies), is not regarded as compliant with data protection law and should not be used.

[3]As per the Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe

2.8. Explicit consent

To the extent that Companies collect and use data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and use such data for OBA, they should first obtain Explicit Consent.

Also, any Company seeking to create or use such OBA segments relying on use of sensitive personal data as defined under Article 8.1 of Directive 95/46/EC will obtain a web user's Explicit Consent, in accordance with applicable law, prior to engaging in OBA using that information. Sensitive personal data, as defined under Article 8.1 of Directive 95/46/EC, represent: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sexi life.

Explicit Consent is defined by the European Industry Self-Regulatory Framework on Data Driven Advertising as "*an individual's freely given specific and informed explicit action in response to a clear and comprehensible notice regarding the collection and use of data for Online Behavioural Advertising purposes*". As a consequence, in order for a company to be compliant, the following conditions must be fulfilled simultaneously:

1. The user must have been informed, in own language and with simple, non-technical wording, that all or most of their browsing activities will be collected and stored, in order to be used later for OBA purposes.

2. The consent must be given specifically for the collection and use of data for OBA purposes (i.e. a company is not compliant if the user gives Explicit Consent to data collection and use, but OBA is not specifically mentioned or is mentioned in an ambiguous manner).

3. Explicit Consent must be freely given, meaning that it must not be induced in any way, by (but not limited to) suggesting users that certain browsing functionalities would not be available or their online experience might be impaired by not consenting.

4. When obtaining Explicit Consent companies must also inform users that the Explicit Consent can be withdrawn at any time:

    a. Users must be provided with an easy to use mechanism to withdraw their Explicit Consent to the collection and use of OBA data;

    b. There must be a clear, dedicated link (i.e. not in the Terms and Conditions or a similar page) from the company's home page to the withdrawal mechanism;

    c. While the wording that should appear on the link is not prescribed, it must be easily understood by the users;

    d. The withdrawal mechanism should be simple and should not ask users for any additional data;

    e. Once the user has withdrawn the Explicit Consent, collection and use of OBA data must stop.

2.9. Best-practice recommendations for self-certification of complianceBest practice recommendation – Advertisers

Advertisers have no specific obligations under the terms of the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR on OBA. However, if the Advertiser, on its own site, permits data to be collected by

Third Parties in order to be used on a web site not under Common Control[4] for OBA purposes, the Advertiser is acting as a Web Site Operator[5], and therefore should provide adequate disclosure of this arrangement. For further details please see Section 2.11 below: Best practice recommendation – Publishers.

Also, while not an obligation in itself, Advertisers should be aware that it is envisaged that the penalties for non-compliant players (Ad Networks, Third Parties, Publishers) are removal of the B2B seal and communication of the failure to comply to the market and the public[6]. It is therefore recommended that signatories acting as Advertisers consider the compliance status of their suppliers when conducting business transactions.

2.10. Best practice recommendation – Agencies

Agencies have no direct specific obligations under the terms of the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR on OBA. Agencies, however, play a key role in serving the Ad Marker; while this does not mean that Agencies take responsibility or assume liability that the Ad Marker will always be served in the correct place, practical considerations may dictate that the Ad Marker is served by the Originating ad server (usually the Agency ad server)[7].

Similar to the situation for Advertisers, while not an obligation in itself, Agencies should be aware that it is envisaged that the penalties for noni compliant players (Ad Networks, Third Parties, Publishers) are removal of the Trust Seal[8] and communication of the failure to comply to the market and the public[9]. It is therefore recommended that signatories acting as Agencies consider the compliance status of their suppliers when conducting business transactions.

2.11. Best practice recommendation – Publishers

The European Industry Self-Regulatory Framework on Data Driven Advertising strongly recommends that Web Site Operators inform Internet users about OBA data collection by Third Parties on their sites. When the company, on its own site(s), permits data to be collected by Third Parties in order to be used on a web site not under Common Control for OBA purposes and the Ad Marker is not provided by these Third Parties, the company provides Adequate Disclosure of this arrangement via a link in the footer, having the following characteristics:

- The link is placed in the footer of all pages, and is distinct from the "Terms and Conditions" link;
- The exact wording of the link itself is not prescribed, but it should be self-explanatory (i.e. the average visitor to the site would understand that by clicking on the link he/she will be redirected to a page where information about data collection on the site is presented)[10];
- A user clicking on the link is presented with an information page containing the following:

---

[4] As defined in the European Industry Self-Regulatory Framework on Data Driven Advertising

[5] As defined in the European Industry Self-Regulatory Framework on Data Driven Advertising

[6] As per the EASA BPR on OBA, principle IV – Compliance and Enforcement Programmes

[7] As defined in the Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe

[8] The Trust Seal is granted by one of the independent Certification Providers selected by the EDAA. Details of the Certification Providers will be published on the EDAA website at www.edaa.eu before the end of 2012.

[9] As per the EASA BPR on OBA, principle IV – Compliance and Enforcement Programmes

[10] Examples of text can be found in the Technical Specifications for implementing the European Industry Self-Regulatory Framework on Data Driven Advertising and EASA BPR in Europe

- A list of Third Parties who are active on the site and with which the user, wittingly or unwittingly, may be interacting;

  OR

- Links to further information on OBA and online privacy such as the OBA User Choice Site;
- Optionally, any other information that supports user understanding and the aims of the European Industry Self-Regulatory Framework on Data Driven Advertising.

3. Notification of self-certification

EDAA will maintain and update, on its website, a list of companies that are selfi certified. As such, once the criteria for self-certification of compliance are fulfilled, companies will notify EDAA via an on-line form, available on EDAA's website. Companies that sign the European Industry Self-Regulatory Framework on Data Driven Advertising or obtain the OBA Icon licence after 1 January 2012 must become compliant and self-certify within 6 months of the signing date.

Contact

info@edaa.eu
European Interactive Digital Advertising Alliance
10-10a rue de la Pépinière,
1000 Brussels
Belgium
www.edaa.eu

4. Frequently Asked Questions

1. What is the deadline to become self-certified?

Companies that have signed the European Industry Self-Regulatory Framework on Data Driven Advertising after 1st of January 2012 must comply within 6 months of adopting the Framework. Companies that participate in the self-regulatory Programme without being a signatory of the European Industry Self-Regulatory Framework on Data Driven Advertising must self-certify within 6 months of signing the Licence Agreements with the EDAA.

2. I am not a Third Party. Do I still need to submit to an independent auditor?

No. The European Industry Self-Regulatory Framework on Data Driven Advertising clearly states, "Companies that are subject to Principle II shall submit to independent audits of their self-certification". Principle II of the European Industry Self-Regulatory Framework on Data Driven Advertising applies to: (a) Third Parties and (b) Companies that "collect and use data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and use such data for OBA".

3. I am not a Third Party. What do I need to do in order to be self3 certified?

In order to be self-certified you have to implement the provisions of the applicable (according to your role in the digital advertising ecoi system) subi section of the *Besti practice recommendations for self-certification of compliance* section.

4. As a Third Party, what do I need to do in order to be self3 certified?

In order to be self-certified you have to implement business processes and, if the case, technologies, to fulfil the provisions of the Criteria for self-certification of compliance section of this document.

5. I am a Third Party as defined in the European Industry Self-Regulatory Framework on Data Driven Advertising. What does self-certification mean for me?

Self-certification is a first step in order to be granted with the Trust Seal certifying that you are compliant with the industry self-regulatory Programme on OBA as per the European Industry Self-Regulatory Framework on Data Driven Advertising.

6. Who grants the Trust Seal?

The Trust Seal is granted by one of the approved Certification Providers selected by the EDAA. Details of the approved certification providers will be available on the EDAA website at www.edaa.eu before the end of 2012.