



Trusted Download Program Requirements

1. DEFINITIONS

(a) Action – means any allegation, investigation, demand, suit, legal proceeding, inquiry, or other legal action, whether formal or informal, initiated by any state or federal governmental authority.

(b) Ad Targeting – The term “Ad Targeting” means the use of Pseudonymous Information to determine User characteristics or preferences for use in advertisement delivery.

(c) Adult Advertisements – are advertisements that are pornographic or sexual in nature; or for products/services that are pornographic or sexual in nature; or advertisements for alcohol, tobacco, firearms or other weapons.

(d) Affiliate – means a person who, for financial consideration, offers the Program Participant’s Certified Software to Users in connection with an Affiliate Distribution Program under a cost per acquisition (pay per install) model and that additionally promotes the Program Participant’s Certified Software to Users using tracking code specific to the Program Participant.

(e) Affiliate, High Control – means an Affiliate that drives web traffic to Participant’s website (usually a landing page) in order to offer Participant’s Software Unit to Users and where the User initiates the download from the Participant’s web site. This distribution method allows the Participant to retain control of the presentation (including surrounding disclosures and context), download, and installation process for its Certified Software.

(f) Affiliate, Medium Control – means an Affiliate that (1) offers Participant’s Software Unit on a site not controlled by the Participant, but (2) in which the Participant controls all required notices, the download file and the install process for its Software Unit (typically via some means of centralized software distribution from web servers owned or controlled by the Participant). This distribution method allows the Program Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is downloaded as part of the software distributed by the Affiliate.

(g) Affiliate Distribution Program – means a process whereby a Participant provides financial consideration to one or more Affiliates in exchange for agreement by the Affiliate(s) to offer Certified Software to Users. Typically, but not always, as part of the process, at least some Affiliates have the Participant’s authorization to hire or subcontract with others to distribute the Participant’s Certified Software to Users.

(h) Agent – means a third party contracted with to perform a business process, provide a service, or deliver a product on behalf of the principal who retained the agent. An agent does not have an independent right to use the relevant User data on its own behalf or in any way other than to perform its obligations on behalf of the principal. Agents include Service Providers meeting these restrictions.

(i) Anonymous Information– The term “Anonymous Information” means information that does not fall within the definition of either Personally Identifiable Information or Pseudonymous Information. “Anonymous information” includes but is not limited to aggregate information.

(j) Applicant – means a company that has submitted Software for Certification to the Program.



Trusted Download Program Requirements

(k) Certification – means the determination by TRUSTe that software submitted to the Program is compliant with the Program Requirements. While Certification applies to software (*i.e.*, the Program does not offer Certification to companies), no company that violates any company-level Program Requirement (such as performing the Prohibited Activities in Section 14) will be eligible for Certification of any of its software.

(l) Certification Date – means the date on which a Participant's Software Unit receives Certification.

(m) Certified Ad Inventory – means the segregated advertisement inventory that may be displayed only to Users of Covered Advertising Software installed after its Provisional Certification Date or Legacy Users of Covered Advertising Software that was installed prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 12.

(n) Certified Covered Advertising Software – means a Participant's Covered Advertising Software that has been tested and awarded Certification, and is currently certified under this Program.

(o) Certified Software – means a Participant's Software Unit that has been tested and awarded Certification, including Provisional Certification, and is currently certified under this Program. Certified Software includes, but is not limited to, Certified Covered Advertising Software and Certified Covered Tracking Software.

(p) Certified Covered Tracking Software – means a Program Participant's Covered Tracking Software that has been tested and awarded Certification, and is currently certified under this Program.

(q) Children's Website – means (as defined in Section 312.2 of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312) a website that, based upon its subject matter, visual or audio content, age of models and other language or characteristics, is targeted or directed to children under the age of thirteen.

(r) Compliance Monitoring – means TRUSTe's monitoring of on-going compliance with these Program Requirements.

(s) Covered Advertising Software – means software that displays advertisements such that the display of any advertisement is not directly triggered by the User's interaction with the Certified Software, unless such advertisements are displayed within the context of the application and the use of any other application is not disrupted. TRUSTe may consider other related formats or methods of delivery as part of the scope of the Program. The User's option to disable display of advertising does not exempt software from this definition. Covered Advertising Software may include Covered Tracking Software where the Covered Advertising Software also meets the definition of Covered Tracking Software.

(t) Covered Tracking Software – means any software that collects a User's web browsing or other information entered into a separate application, where a purpose is to transfer such information to a destination off the User's computer that is not controlled by the User. Covered Tracking Software does not include software where the collection and transfer purposes are network integrity or functionality, application integrity, or information security. TRUSTe may exclude, in its sole discretion, software where the purpose is the backup of and/or



Trusted Download Program Requirements

increased access to the information by the user. To be eligible for this exception, the user's data/information cannot be used for advertising, marketing, profiling, personalization or related activities. (Covered Tracking Software may include Covered Advertising Software where the Covered Tracking Software also meets the definition of Covered Advertising Software.)

(u) Default Option – means an option that is pre-selected, so that a User can accept the option without taking any additional affirmative action indicating consent. For purposes of this definition, allowing Users to accept an option by selecting the “Enter” key on their computer keyboards does not indicate affirmative consent.

(v) Distribution Bundle, High Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously to Users by a Distribution Partner, in which the Participant controls the download, the Reference Notice(s), and the install process for its Software, typically by means of centralized software distribution from web servers owned or controlled by the Program Participant. Participant must have a contract in place with the Distribution Partner that requires the Distribution Partner to use the TDP-approved Primary Notice during the download/installation process. This distribution method allows the Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is consistently downloaded as part of the Distribution Bundle.

(w) Distribution Bundle, Medium Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously to Users by a Distribution Partner, in which the Participant does not directly control the download and install process for its Software Unit, but has a contract in place with the Distribution Partner requiring that the Distribution Partner not violate the TDP Program Requirements.

(x) Distribution Partner - means a person that, for financial consideration, distributes Software to Users on behalf of the Program Participant. Typically, but not always, the Distribution Partner includes their own software and/or software from third parties as part of a Distribution Bundle offered to Users.

(y) Effective Date – means the date this Agreement is signed by both parties, or, in the case of a Renewal, the day after the previous license expires, if the requirements for Renewal are satisfied.

(z) EULA – means an End User License Agreement.

(aa) Informed Third Party – means an entity that Participant has designated in writing to TRUSTe to receive Certification status updates, including: failure to obtain Certification, Certification of the Software, placement on the Whitelist, placement on Probation or Suspension status, removal from the Whitelist, and/or termination from the Program.

(bb) Just in Time Notice – means notice of a functionality that is added after a User has already consented to install Software but just prior to the execution of that functionality. When this happens, a User is provided with Primary Notice of the new functionality and given the opportunity to provide consent just prior to execution of that functionality. Waiting until just prior to execution of certain functionalities can provide the User with better context to make certain consent decisions. While the Program permits the use of Just in Time Notice for some Certified Software, the Program does not permit its use for Certified Covered Advertising



Trusted Download Program Requirements

Software. Just in Time Notice may not be used where such use would negatively impact the original value proposition of the Certified Software, as determined by TRUSTe.

(cc) Legacy User – means all Users who have installed a Participant’s Certified Software before the Certification Date of such software and who received disclosures not substantially similar to those in Sections 3 and 5 of these Program Requirements.

(dd) Market Research – The term “Market Research” means the use of Pseudonymous Information to understand how Users are using their computers and the Internet.

(ee) Material Change(s) – means a substantive change that would be of importance or consequence to the User, which may include:

(i) Changes to privacy practices, meaning changes relating to:

- (1) Practices regarding notice, disclosure, and use of Personally Identifiable Information and/or Third Party Personally Identifiable Information,
- (2) Practices regarding user choice and consent to how Personally Identifiable Information and/or Third Party Personally Identifiable Information is collected, used and shared, or
- (3) Measures for data security, integrity, or access.

(ii) Modifications to Certified Software that are relevant to these Program Requirements, including but not limited to:

- (1) Changes to one or more functionalities that are required to be disclosed per Sections 3, 5, 6, 7, 10 and 11 of these Program Requirements, and/or;
- (2) Changes to the way any required functionalities are disclosed, including but not limited to changes to wording, font, size and/or order of the disclosures, and/or;
- (3) Changes to the Software’s method or means of storing data remotely.

(iii) Material update or substantive revision to Certified Software functionality including but not limited to: Substantive additions, reconfigurations, re-architecture and/or changes to Software functionality;

(iv) Material Changes do not include any changes which solely affect the performance or integrity of the Software Unit, such as increases in speed, reliability, or information security.

(ff) Non-Certified Ad Inventory – means the segregated ad inventory that is displayed to Legacy Users of Covered Advertising Software that have not received the notice and/or given the consent required under Section 12.

(gg) Notice(s) – means the Primary Notice and the Reference Notice, together and individually.



Trusted Download Program Requirements

(hh) Online Preference Marketing (or OPM) – means a process whereby data are typically collected over time and across web pages to determine or predict User characteristics or preferences for use in ad delivery on the web. The OPM process can use Pseudonymous Information or a combination of Personally Identifiable Information and Pseudonymous Information.

(ii) Participant – means a company that has software that is currently certified or provisionally certified in the Program and has executed a signed agreement with TRUSTe.

(jj) Personally Identifiable Information (or PII) – means any information (i) that identifies or is used to identify, contact, or locate the person to whom such information pertains or (ii) from which identification or contact information of an individual person is derived. Personally Identifiable Information includes, but is not limited to: name, address, phone number, fax number, email address, financial profiles, medical profile, social security number, and credit card information. Additionally, to the extent unique information (which by itself is not Personally Identifiable Information) such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address is associated with Personally Identifiable Information, then such unique information also will be considered Personally Identifiable Information. Notwithstanding the above, Personally Identifiable Information does not include information that is collected anonymously (*i.e.*, without identification of the individual user) or demographic information not connected to an identified individual. Personally Identifiable Information includes Third-Party Personally Identifiable Information.

(kk) Primary Notice – means information presented to each user in a manner that is clear, prominent and unavoidable, and designed to catch the User's attention during the Software Unit(s) installation. The Primary Notice must be fully visible to a User without additional action on the part of the User, such as having to scroll down the page to reach the beginning of the required disclosures. Primary notice may be presented using Just in Time Notice, except in the case of Certified Covered Advertising or Tracking Software. The Primary Notice cannot be displayed after the software is installed, as the last step in the installation process. In cases of platform-specific technical limitations, TRUSTe may, in its sole discretion, permit the Primary Notice to be presented after installation but prior to activation.

(ll) Program – means the TRUSTe Trusted Download Certification Program.

(mm) Program Requirements – means the requirements for participation in the Program as specified in this Schedule A, as may be amended from time to time.

(nn) Provisional Certification – means an interim level of Certification of a Participant's Software Unit, during which time the Program Participant will be subject to all requirements that apply to its Certified Software as well as certain additional requirements, including, as relevant, those specified in Section 11(c).

(oo) Provisional Certification Date – means the date on which a Participant's Software Unit receives Provisional Certification, or is transitioned from full status to Provisional status, pursuant to Section 11.

(pp) Provisionally Certified Software – means a Software Unit that has received Provisional Certification.



Trusted Download Program Requirements

(qq) Pseudonymous Information – The term “Pseudonymous Information” means information that may correspond to a person, account or profile but is not sufficient, either on its own, or through combination with other easily accessible public information, to identify, contact, or locate the person to whom such information pertains. Examples include but are not limited to a User’s IP address, machine ID, and the web pages a User views.

(rr) Reference Notice – means information that is easy to locate (e.g., via an easily accessible scroll box or a prominent and clearly labeled link) and easy to read and comprehend. Examples of Reference Notices include Privacy Statements and End User License Agreements (EULAs).

(ss) Service Provider(s) – means a third party that performs or assists in the performance of a function or activity involving the use or disclosure of Personally Identifiable Information or Third Party Personally Identifiable Information.

(tt) Software Disclosures – means the statements made in the Self-Assessment in regard to the Software Unit.

(uu) Software Unit – means the software described in Exhibit 1 that is to be tested and reviewed for Certification by TRUSTe.

(vv) Third-Party Personally Identifiable Information (or “Third-Party PII”) - means Personally Identifiable Information that is collected by a Program Participant from a User other than the User to whom it pertains, or whom it identifies.

(ww) TRUSTe Marks – means collectively the registered certification marks and trademarks of TRUSTe.

(xx) User – means an authorized user or owner of a computer on which a Software Unit is installed.

(yy) Whitelist – means the public list maintained by TRUSTe of all Certified and Provisionally Certified software, and the associated Participants that are currently in the Program.

2. Program Management

(a) Certification. The process of certifying software for compliance with the Program Requirements shall be as provided for below:

(i) Certification shall apply to an individual Software Unit. Participant shall provide TRUSTe with a description, unique identifier and an archival format for each Software Unit it wishes to certify. Participant shall provide TRUSTe with all documentation, whether in written, electronic, or other appropriate format, reasonably requested by TRUSTe in connection with the Certification process. Such documentation shall include a completed Self-Assessment Form and other information about the Software as may be reasonably requested by TRUSTe.

(ii) Once Participant has submitted its application, no Material Change is permitted, without written notice to TRUSTe. Any Material Change may trigger restarting the Certification process at TRUSTe’s discretion.

(iii) TRUSTe shall review the Self-Assessment and test the Software Unit for compliance with the Program Requirements. A Certification decision, and corresponding report



Trusted Download Program Requirements

or reports summarizing TRUSTe's findings, will be provided to the Participant. If TRUSTe does not certify the Software, Participant shall be permitted 30 days time to remedy the failure and resubmit the Software for Certification, whereupon TRUSTe shall provide a second review and test process, and a second report and Certification decision.

(b) Material Changes. Any Material Change to the Certified Software may trigger the need for recertification of the Software, which may require additional fees as provided for herein. TRUSTe will respond to all requests made by Participants to review Material Changes within five (5) business days of receipt of notice of the requested Material Change.

(c) Participant Obligations. During the Term hereof, and solely with respect to the Software Units for which it seeks certification, the Participant shall:

(i) Make no Material Change to any features, functions, characteristics, architecture, or coding of the Software, in a manner affecting its compliance with the Program, without 1) notifying TRUSTe in writing of Participant's intent to do so, and 2) obtaining TRUSTe's written decision as to whether such change triggers a recertification requirement;

(ii) Provide written notice to TRUSTe on a quarterly basis of any non-material changes to the software that had taken place during the previous quarter, including updates to the Certified Software version number, if applicable;

(iii) Immediately notify TRUSTe in writing of any Material Change in the Software Unit or in the circumstances or facts that initially served as a basis for Certification, or which are otherwise related to Program compliance;

(iv) Immediately provide notice in writing to TRUSTe of any change in the name of a Software Unit or change in the Participant's name

(v) Except to the extent prohibited by law, provide notice to TRUSTe of any private lawsuit or Action against it or the Certified Software by any person, law enforcement, or other governmental entity in any country, related to Participant's activities connected to the Program or to the Program Requirements. Such notice shall be provided within five (5) business days of learning of such private lawsuit or Action;

(vi) Cooperate with TRUSTe during TRUSTe's Compliance Monitoring and audit activities;

(vii) Continually provide updated complaint contact information to TRUSTe;

(viii) Make its software compatible with virtualization tools, such as VMWare, such that TRUSTe is able to run the Participant's software in a virtualization tool

(ix) Make no representations to anti-spyware vendors that the TRUSTe's whitelist supercedes or replaces vendors' own independent testing and evaluation processes or that such processes should consider only or primarily the product's whitelisted status with TRUSTe

(d) TRUSTe Obligations. TRUSTe shall within a reasonably prompt period of time:

(i) Test the submitted Software Unit for compliance with the Program Requirements;



Trusted Download Program Requirements

(ii) Provide a pass/fail decision, as well as a report, regarding the Software Unit to the Participant;

(iii) Retest and provide a second report, as well as a second pass/fail decision, if necessary; and

(iv) Provide on-going Compliance Monitoring for Software in the Program, to the extent provided for in these Program Requirements.

(e) Whitelist. TRUSTe may, but is not required to, maintain a list of all current Software and/or Participants that are members of the Program ("Whitelist"). Participant hereby consents to the use of its name and the name of the Certified Software on any Whitelist compiled by TRUSTe during the Term. TRUSTe may also, on its Whitelist, site, consumer dispute resolution process, or in response to inquiry, disclose whether Participant and/or the Software Unit is a member of the Program and how the Software Unit is categorized under Program definitions.

(f) Dispute Resolution. Participants must participate in TRUSTe's Watchdog process to resolve non-frivolous, as defined by TRUSTe, privacy concerns or complaints related to Certified Software raised by Users. TRUSTe will act as a liaison between the Participant and the consumer to resolve relevant inquiries, including recommending or requiring corrective action where necessary, as pertaining to these Program Requirements.

(g) Updates to Informed Third Parties. TRUSTe will provide on-going Certification status updates, including the status of monitoring and enforcement activities if applicable, as necessary to Informed Third Parties, if any.

(h) Applications in Languages Other Than English. All Software for which Participant is seeking Certification hereunder must have all User-facing statements written entirely in the English language, unless Participant follows translation guidelines described in this provision with TRUSTe's approval. If the Participant wishes to extend certification of an application to versions in languages other than English, the Participant agrees to:

(i) If the application is in English and User-facing statements are in another language, translate the User-facing statements into another language by an accredited translation company that is approved by TRUSTe.

(ii) If both User-facing statements and the application are in another language, the Participant will submit the application for testing and certification

3. Notice. The Program Requirements adopt a layered-notice approach.

(a) The Primary Notice. The Primary Notice, which is required of all certified applications, at a minimum must have a link to the reference notice. Primary notice may be presented using Just in Time Notice, except in the case of Certified Covered Advertising Software. The intent of this provision is to ensure that material terms are clearly presented prior to the execution of the value proposition. If any of the functionality described in Sections 3(a)(i) through 3(a)(iii) is present, this Primary Notice must include the following information:

(i) For all Certified Software:



Trusted Download Program Requirements

- (1) Whether installing the software, alone or as part of a bundle, may:
 - A. Redirect the User's Internet searches;
 - B. Add a toolbar to the User's web browser or modify other functionality of the browser or desktop as determined by TRUSTe;
 - C. Change the User's home page, default search provider or error page handling or otherwise modify browser settings as determined by TRUSTe;
 - D. Change the User's default provider, web proxy, security or other changes to Internet settings as determined by TRUSTe; or
 - E. Cause known material adverse effects on system performance for typical Users as determined by TRUSTe.
 - (2) A prominent link to all applicable Reference Notices.
- (ii) In addition, for all Certified Covered Advertising Software:
- (1) The name of the Program Participant.
 - (2) The essence of the proposed exchange, including (as applicable):
 - A. The name or brand of the Certified Covered Advertising Software, and if the Certified Covered Advertising Software is bundled with other software (and if such other software has a separate name or brand), the name or brand of the other software;
 - B. Whether the Certified Covered Advertising Software will perform collection and transfer of information to a computer not under the User's control for the purpose of targeting advertisements and/or Market Research.
 - C. That advertisements will be displayed and a brief indication of the types of advertisements displayed and when advertisements will be displayed. As applicable, disclose that the advertisements will appear only while Users are using software in which the Certified Covered Advertising Software is integrated, while they are online generally, or at other specified times; and
 - D. If applicable, that the software will display Adult Advertisements.
- (iii) In addition, for all Certified Covered Tracking Software:
- (1) The name of the Program Participant.
 - (2) The essence of the proposed exchange, including (as applicable):



Trusted Download Program Requirements

- A. The name or brand of the Certified Covered Tracking Software, and if the Certified Covered Tracking Software is integrated into or bundled with other software (and if such other software has a separate name or brand, the name or brand of such other software);
 - B. When the collection and transfer of information to a computer not under the User's control for the purposes of Ad Targeting and/or Market Research will occur. As applicable, disclose that the collection and transfer of information to a computer not under the User's control will occur only while Users are using the Certified Covered Tracking Software, while they are online generally, or at other specified times.
- (b) The Reference Notice. The Reference Notice must, at a minimum, include:
 - (i) For All Certified Software:
 - (1) All of the information contained in the Primary Notice, except that it is not necessary to have EULAs and/or Privacy Statements tailored to each means of distribution; and
 - (2) Instructions on how to uninstall the software, as provided for in Section 7.
 - (3) Whether installing the software, alone or as part of a bundle, may leave tracking assets such as cookies, files, or registry entries that are referenced or active after uninstall, by the Participant or other 3rd parties and:
 - A. the purpose of any such tracking assets; and
 - B. whether any such tracking assets are accessible by third-parties via other web sites or programs.
 - (ii) In addition, for all Certified Covered Advertising Software:
 - (1) A description of the types and frequency of the advertisements displayed by the software;
 - (2) If applicable, that the software will display Adult Advertisements and an explanation of how Users can manage their computers to make sure that children are not served with advertisements from Certified Covered Advertising Software installed by adults;
 - (3) If applicable, that the software will display Adult Advertisements, and disclosure that software should be installed only by Users age eighteen (18) and over; and
 - (4) Information, including a link, on how to access the Program Participant's website and customer support mechanism.
 - (iii) In addition, for all Certified Covered Tracking Software:



Trusted Download Program Requirements

- (1) Information, including a link, on how to access the Participant's website and to the Participant's customer support mechanism.

4. Consent to Install. Participants must provide Users with a means to give their consent to install the Participant's Certified Software prior to the completion of any such installation. The consent mechanism must meet the following standards:

- (a) For all Certified Software:
 - (i) Users must be given a means to indicate their consent to install the Certified Software after receiving all applicable Primary Notices;
 - (ii) The language used to describe Users' options to consent to install Certified Software must be plain and direct;
 - (iii) Installation of software shall not proceed if a User declines consent to install the Certified Software or closes the dialog box containing the consent option; and
 - (iv) Users may only be asked once in any installation process to reconsider their decision not to install software or to close the dialog box with the consent option, unless Users have indicated it is acceptable to ask them later.
- (b) In addition, for all Certified Covered Advertising Software and Certified Covered Tracking Software:
 - (i) The option to consent may not be the Default Option; and
 - (ii) The option to decline installation must be of equal prominence to the option to provide consent for installation.

5. Notice and Choice Requirements for Uses of PII and Pseudonymous Information.

- (a) Primary Notice. If PII or Pseudonymous Information is collected and transferred to a computer not under the User's control through the Certified Software, the following information must be provided in a Primary Notice:
 - (i) For all Certified Software: at least one reference notice linked from the Primary Notice must include information about choices available to them regarding their data.
 - (ii) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software: A description of the PII collected or transferred to a computer not under the User's control through the Software Unit, the uses of PII obtained through the Certified Software by Participant, and the types of companies to which Participant will transfer PII.

With TRUSTe's prior approval, certain information required by this provision to be included in the Primary Notice, may be moved to a "learn more about this" link, as long as all required disclosures are complete, clear, prominent and unavoidable, in TRUSTe's sole judgment and discretion.

- (b) The Reference Notice. If PII or Pseudonymous Information is collected through the Certified Software, the Reference Notice must include at least the following:
 - (i) For All Certified Software:



Trusted Download Program Requirements

- (1) Whether the software collects PII, and if so, the following additional disclosures:
 - A. What PII is being collected;
 - B. The identity (including name, address and e-mail address) of the entity collecting such information;
 - C. How such information will be used;
 - D. A description of the types of entities with whom the information is shared, if at all;
 - E. The purposes for which data is disclosed to third parties;
 - F. How and when the User may exercise choice, as required in Section 5(c), below;
 - G. Whether Users' PII will be supplemented with information from other sources;
 - H. The User's access rights to correct material inaccuracies in Personally Identifiable Information, such as account or contact information; and
- (2) A general statement describing data security practices. Program Participant must implement reasonable procedures to protect Personally Identifiable Information and/or Third Party Personally Identifiable Information within its control from unauthorized use, alteration, disclosure, distribution, or access. Program Participant shall utilize appropriate, commercially reasonable means, such as encryption, to protect any sensitive information, such as social security numbers, financial account and transaction information, and health information that it collects.
- (3) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software:
 - A. Whether the Certified Software collects Pseudonymous Information, and if so, the following additional disclosures:
 - I. The types of Pseudonymous Information collected by the Certified Software;
 - II. The Participant's use of Pseudonymous Information;
 - III. Whether the Participant shares Pseudonymous Information with Third Parties and if so, what restrictions the Program Participant places on its further use or dissemination;

(c) Choice Requirements.



Trusted Download Program Requirements

- (i) For All Certified Software:
 - (1) The User to whom PII pertains must be offered an opt-out choice if PII collected through the software may be used in the following ways:
 - A. Use not related to the primary purpose for which the User provided it. The scope of use deemed related to the primary purpose shall be defined in the Reference Notice and shall be reasonable to Users;
 - B. Disclosure or distribution to third parties, other than Agents; or
 - C. Merger of Pseudonymous Information with previously collected PII on a going forward basis (*i.e.*, after the user provides PII) for use in Online Preference Marketing, where such use had not been previously disclosed to and accepted by the User.
 - D. Certified Software Providers may require the collection or use of PII as part of the value proposition of the software, and may decline to provide the software if User opts out from such use.
 - (2) The User to whom PII pertains must be provided with notice and provide his or her affirmative consent prior to the merger of PII with Pseudonymous Information previously collected through the software for use in Online Preference Marketing.
 - (3) Before Third-Party PII collected through the software may be used or disclosed for any purpose other than the primary purpose for which such information was collected, the person to whom such information pertains must provide affirmative consent. [Notwithstanding such restriction, such information (i) may be disclosed pursuant to legal process (*e.g.*, subpoenas, warrants) or (ii) may be used to send a one-time e-mail message to the person to whom the information pertains in order to solicit such opt-in consent.] Prohibited behavior includes, but is not limited to the use of Third-Party PII collected through the software (*e.g.*, via an address book) to send unsolicited bulk communications to third parties.

6. Special Requirements for Certified Covered Advertising Software. Consumers should be able to understand why they receive advertisements from a Participant. To this end, Certified Covered Advertising Software must comply with the following additional requirements:

(a) Reaffirmation. Before the User receives an advertisement, Certified Software must display an information notice, in a clear, prominent, and unavoidable fashion: (i) demonstrates a representative example of the Certified Software's advertisements, (ii) provides the User with more information on how the Certified Software functions, and (iii) provides



Trusted Download Program Requirements

information on how to uninstall the software, which may be provided via a prominently labeled link. When a Covered Advertising Software provider has more than one format, a representative example may be used, provided that the example is sufficient to enable a reasonable User to make an informed decision.

(b) **Branding.** Advertisements displayed by Certified Covered Advertising Software must be branded with, or within close proximity to, the name of the Participant and the brand of the Certified Software (if distinct from the name of the Participant).

(c) **Co-Branding.** The mechanism displaying the advertisement must also contain, on its face:

(1) The name of the Certified Software;

(2) The software or content the User downloaded as a requirement to get the Certified Software; and

(3) A prominently and clearly labeled link to additional information. The additional information page must include:

A. A representative list of the content that cause the display of such advertisements, if applicable; and

B. The estimated frequency of advertising that a User can reasonably expect; and

C. A list of web-based content available to the user when the Certified Software is installed; and

D. Clear instructions for removal of the Certified Software.

7. **Uninstall.** Certified Software must provide Users with an easy and intuitive means of uninstallation. In addition, the following uninstall requirements apply.

(a) For all Certified Software:

(i) The name of the Certified Software must be listed in the customary place for user initiated uninstall within the software platform (e.g., an Add/Remove Programs facility in the Windows operating system);

(ii) Commercially reasonable efforts need to be made to ensure Certified Software and associated files are removed from Users' computers. Understanding that there are legitimate exceptions, TRUSTe may approve exceptions, at its discretion, in cases such as:

(1) Uninstallation of Certified Software may be conditioned on the uninstallation of other software on a User's computer (for example, uninstallation of Certified Covered Advertising Software may be conditioned on the uninstallation of other software that is bundled with the Certified Covered Advertising Software), provided that the other software meets the uninstall requirements of this section;



Trusted Download Program Requirements

- (2) TRUSTe recognizes that Certified Software may require the User to install other software (e.g., Adobe Acrobat, Flash), and that the other software may legitimately remain on a User's computer after uninstallation of the Certified Software;
- (3) Because the User has installed software program(s) that also require the use of the other software in order to function;
- (4) Because properly disclosed anti-fraud or distribution accounting measures (e.g. identifying which distributor is responsible for the download) require leaving behind assets, for example, to verify that a machine is not making unauthorized reinstallation of software that can only be installed once per machine;
- (5) Creation of material data asset that the consumer may want, even after software uninstall, such as email files being left behind after uninstall of an email client application;
- (6) TRUSTe, in its sole discretion, will determine whether other software or other files left behind after uninstallation are for a legitimate reason.

(iii) Once a User has uninstalled Certified Software, the Certified Software may not reinstall on a User's computer unless the reinstallation is performed pursuant to the Program Requirements and, in particular, pursuant to new consent;

(iv) Uninstall instructions for all Certified Software must also be available from the Participant's web page either directly or through a link; and

(v) No PII shall be required in order to uninstall Certified Software unless the PII was previously collected in compliance with the Program, and it is reasonably necessary, and only used to authenticate and/or identify the User.

(b) In addition, for all Certified Covered Advertising Software, uninstallation instructions must be available in multiple places that are easy for Users to find, including:

(i) By a link from the advertisements themselves, or from the browser window or frame where such content is provided; and

(ii) On the Participant's website as a standalone item in an easily discoverable location (for example, in a customer support, FAQ, or similar section.)

(c) In addition, for all Certified Covered Tracking Software uninstallation instructions must be available in multiple places that are easy for Users to find, including:

(i) On the Participant's website as a standalone item in an easily discoverable location (for example, in a customer support, FAQ, or similar section)

8. Software Updates.

Participants must give Users Primary Notice of changes and an opportunity to uninstall prior to applying any Material Changes to the Certified Software of existing Users. Material Changes that are solely performance related code changes that do not change underlying functionality may be exempted from this requirement at TRUSTe's discretion. Changes to installed Certified



Trusted Download Program Requirements

Software that would transform it into Covered Advertising Software or Covered Tracking Software must be treated as a new Software Unit under these Program requirements.

9. Third-Party Distribution / Affiliate Practices.

For all Certified Covered Advertising Software and Certified Covered Tracking Software; and certain other Certified Software, as determined by TRUSTe, who distribute Software Units via Distribution Partners or Affiliate Distribution Programs; Participants must:

(a) Have contractual provisions in place with such Distribution Partners and Affiliates prohibiting them from causing Participant's Certified Software to not comply with these Program Requirements. In the context of an Affiliate Distribution Program, the contract between the Program Participant and its Affiliate must further require that contracts between the Affiliate and its subcontractors bind the subcontractors to comply with these Program Requirements;

(b) Disclose to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the names of Distribution Partners and Affiliates as well as locations (e.g. URLs of affiliates within an Affiliate Distribution Program) where such Distribution Partners and Affiliates provide or drive traffic to Certified Software to consumers so that such third-party distribution and affiliate practices may be reviewed, tested, and monitored for compliance with these Program Requirements and related legal standards;

(c) Disclose to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the modifications that Distribution Partners or Affiliates are permitted to make to Certified Software as well as locations where Distribution Partners and Affiliates provide such modified Certified Software to Users so that such modifications may be monitored for compliance with these Program Requirements;

(d) Demonstrate to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, that Participant has an effective process for ensuring that Distribution Partners and Affiliates are not engaging in practices that contribute to Participant's non-compliance with these Program Requirements;

(e) Evaluate, on an on-going basis, Distribution Partners and Affiliates for deceptive or other behavior that contributes to Participant's non-compliance with these Program Requirements, and report any known substantive non-compliance with these Program Requirements involving Certified Software. Failure to report any such non-compliance in a timely manner shall be grounds for a suspension or termination of a Participant from the Program and de-certification of all or any of such Program Participant's Certified Software; and

(f) If the Program Participant learns that a Distribution Partner or Affiliate has engaged in practices that materially violate these Program Requirements, the Program Participant must follow the Program's specified re-opt-in procedures (as specified in Section 12 of these Program Requirements) to re-opt in at least one User of each computer that may have received the Certified Software by those means.

10. Additional Protections for Children. Participants with Certified Covered Advertising Software or Certified Covered Tracking Software must take the following steps:

(a) Prevent the distribution of their Certified Software on Children's Websites, including by prohibiting their Distribution Partners and Affiliates from such distribution;



Trusted Download Program Requirements

(b) Engage in commercially reasonable oversight to determine where advertisements promoting the installation of their Certified Software appear;

(c) If their Certified Covered Advertising Software delivers Adult Advertisements, Participants must ensure that such advertisements are branded so that they may be recognized by child protection software filters by either:

(i) including the phrase "for adults 18 years" in text somewhere on the face of the Covered Advertisement, or

(ii) including the phrase "for adults 18 years" in the meta keyword tag for the page containing the Covered Advertisement, or

(iii) including the phrase "for adults 18 years" within the "alt", "name" or "id" attribute of the image tags within the Covered Advertisement.

11. Provisional Certification. In certain cases, additional transparency may be useful to companies considering partnerships with Participants and to consumers considering downloading the Participant's application. In order to provide such additional transparency, Program Applicants that would otherwise be entitled to Certification of their Software shall have their Software be eligible only for Provisional Certification.

(a) Certified Software with Legacy Users addressed in Section 12 of these Program Requirements are eligible only for Provisional Certification until all required steps are completed.

(b) Provisional Criteria - At TRUSTe's discretion, TRUSTe may designate a Participant's Certified Software as Provisionally Certified if other substantial risk factors are present, that pertain to the Participant's online practices, and that call into question the credibility of the Participant. TRUSTe will provide notice to the Participant and a reasonable opportunity to respond. Risk factors may include, but are not limited to:

(i) Practicing any of the Prohibited activities listed in Section 14 of these Program Requirements within 24 months before submitting application into the Program.

(ii) Credible allegations of deceptive or abusive practices online within 24 months before submitting application into the Program.

(iii) Resolution of government action within the past 3 years before submitting application into the Program indicating deceptive or abusive online practices, including actions by a States Attorney General, the Federal Trade Commission (FTC), a Court, or other government agency.

(iv) Current (or former) TRUSTe client in the Web Privacy Seal Program, who is not in good standing with TRUSTe.

(c) Provisional Requirements - Participants with Provisionally Certified Software will be subject to the following:

(i) Notwithstanding any written consent obtained pursuant to Section 2(a) of the Agreement, Program Participants with Provisionally Certified Software may not mention their software's Certification in any manner without including the qualification "Provisional."



Trusted Download Program Requirements

(ii) Participants with Provisionally Certified Software may be subject to additional Compliance Monitoring or reporting requirements as determined by TRUSTe.

(iii) Provisionally Certified Software will be so designated on a webpage maintained by TRUSTe.

(iv) Provisionally Certified Software will be so designated on any Whitelists maintained by TRUSTe.

(d) Fully Certified Software not certified as Provisional may become Provisional if:

(i) Participant violates Program Requirements and does not correct in a timely manner as determined by TRUSTe;

(ii) Participant's affiliate programs or dealings with merchants, and advertisers related to the Certified Software are conducted in a fraudulent or abusive manner; or

(iii) Participant becomes the subject of a publicly filed proceeding and/or settlement by the Federal Trade Commission, State Attorneys General, or similar body for a matter related to these Program Requirements.

(e) Eligibility for Full Certification. Participants with Provisionally Certified Software will be eligible for full Certification of their compliant Software Unit(s) upon the last to occur of the following:

(i) Six (6) months following the Certification Date;

(ii) Resolution of the concerns that lead to the Provisional Certification to TRUSTe's satisfaction, including a written attestation of fulfillment of TRUSTe's requirement

(iii) Satisfaction of the requirements described in Sections 12 and 13, if applicable.

(f) Warrant that all new installations meet TDP Requirements. Upon meeting all Program Requirements, the Applicant must warrant that on an ongoing basis all new installations of Provisionally Certified software will continue to meet the Program Requirements, as of the Provisional Certification Date.

(g) Segregate advertising inventory. Participants with Provisionally Certified Software that serves advertising, shall be required to do the following:

(i) Immediately segregate the advertising inventory that is displayed to its Users into two distinct sets: Certified Ad Inventory and Non-Certified Ad Inventory.

(1) Certified Ad Inventory shall be inventory that is displayed to Users who installed the Provisionally Certified Software after the Provisional Certification Date (and thus compliant with these Program Requirements) or displayed to Users who installed Provisionally Certified Software prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 12 below.



Trusted Download Program Requirements

- (2) Non-Certified Ad Inventory shall be inventory that is displayed to Legacy Users of Provisionally Certified Software who had not received the notice and/or given the consent required under Section 12 below.

(ii) Explicitly make available to advertisers the ability to purchase only Certified Ad Inventory described in Section 11(g)(i)(1) above.

(iii) Ensure that no advertisements from Registered Program Advertisers appear within Non-Certified Ad Inventory.

12. Message Legacy Users. Within six (6) months of the Provisional Certification Date, the Program Participant must initiate the re-opt-in process of their Legacy Users, and must completely re-opt in such Legacy Users within one (1) year. Legacy Users must be given a notice describing the material facts about the operation of the software and an opportunity to provide consent to continue to have Provisionally Certified Software on their systems or to uninstall the Provisionally Certified Software. The option to provide consent may not be the Default Option. Users who decline consent or who close the dialog box shall be promptly provided with uninstall instructions. The software cannot serve ads to any User who subsequently fails to uninstall the software.

13. Evaluator Requirement - Participants and Program Applicants that meet the following criteria may be required to submit to an evaluation of their compliance with the Program.

(i) Evaluation Criteria:

- (1) If Program Applicant asserts that one or more of its Legacy Users were acquired in compliance with these Program Requirements as per Section 12, TRUSTe may require that they submit to an evaluation of the methods and procedures used in making that determination.
- (2) If Program Applicant or Participant currently distributes their Covered Advertising Software or Covered Tracking Software with one or more Medium Control Affiliates, TRUSTe may require that the Program Applicant or Participant submit to an evaluation of the business practices for each of the Program Applicant's or Participant's Affiliates and all Distribution Partners as they reasonably pertain to these Program Requirements.
- (3) If Program Applicant or Participant currently is, or within the past three (3) years was, under investigation by Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an evaluation of all business practices that reasonably pertain to these Program Requirements.
- (4) If Program Applicant or Participant is, or becomes the subject of a publicly filed proceeding and/or settlement by the Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an



Trusted Download Program Requirements

evaluation of all of its business practices that reasonably pertain to these Program Requirements.

(ii) Evaluation Scope

- (1) The evaluations are to be performed by, in TRUSTe's discretion, either TRUSTe or a firm chosen by the Program Participant and deemed suitable by TRUSTe.
- (2) The results of the evaluation shall be confidential, provided that the top-level results of all evaluations shall be provided to TRUSTe upon completion.
- (3) In all instances, TRUSTe reserves the right define the scope of the evaluation.

14. Prohibited Activities. All Participants shall not, and shall take steps in accordance with Section 9 to ensure that their Distribution Partners and Affiliates do not, do any of the following:

- (a) Take control of a User's computer by deceptively:
 - (i) using the computer to send unsolicited information or material from the computer to others;
 - (ii) accessing, hijacking or otherwise using the computer's modem or Internet connection or service and thereby causing damage to the computer or causing the owner or authorized User, or a third party defrauded by such conduct, to incur charges or other costs that is not authorized by the owner or User;
 - (iii) using the computer as part of an activity performed by a group of computers that causes damage to another computer;
 - (iv) delivering advertisements that a User cannot close without turning off the computer or closing all other sessions of the Internet browser for the computer; or
 - (v) using rootkits or other software that are typically used to hack into a computer and gain administrative-level access for unauthorized use of a computer.
- (b) Modify security or other settings of the computer that protect information about the User for the purposes of causing damage or harm to the computer or the User.
- (c) Collect PII through the use of a keystroke logging function or other deceptive means without authority of the owner of the computer.
- (d) Induce the User to provide PII to another person by intentionally misrepresenting the identity of the person seeking the information. This includes inducing the disclosure of information by means of a web page or Software Unit that:
 - (i) is substantially similar to a web page or Software Unit established or provided by another person; and
 - (ii) misleads the User that such web page or Software Unit is provided by such other person.



Trusted Download Program Requirements

(e) Induce the User to install the Software onto the computer, or prevent reasonable efforts to block the installation or execution of, or to disable the Software, by:

(i) presenting the User with an option to decline installation but, when the option is selected by the User or when the User reasonably attempts to decline the installation, nevertheless proceeding with the installation;

(ii) misrepresenting that the Software will be uninstalled or disabled by a User's action, with actual or constructive knowledge that the Software will not be so uninstalled or disabled;

(iii) causing software that the User has properly removed or disabled to automatically reinstall or reactivate on the computer;

(iv) changing or concealing the name, location or other designation information of the software for the purpose of preventing a User from locating the software to remove it;

(v) using randomized or intentionally deceptive file names, directory folders, formats or registry entries for the purpose of avoiding detection and removal by a User;

(vi) causing the installation of software in an inappropriate computer directory or computer memory location for the purpose of evading a User's attempt to remove the software;

(vii) requiring completion of a survey, or disclosure of PII, to uninstall software;

(viii) requiring, without the authority of the owner of the computer, that a User obtain a special code or download a third-party program to uninstall the software; or

(ix) intentionally causing damage to or removing any vital component of the operating system when uninstallation is attempted.

(f) Misrepresent that installing software or providing log-in and password information is necessary for security or privacy reasons unrelated to the software itself, or that installing software is necessary to open, view or play a particular type of content online or offline (e.g., can not falsely state software is necessary for accessing web site).

(g) Induce the User to install, download or execute software by misrepresenting the identity or authority of the person or entity providing the software to the User. This includes, but is not limited to use of domains with misspelling of frequently visited web sites (*i.e.*, 404 squatting), the use of deceptive or misleading inducements or text or other creative elements to lure a consumer to a website, etc.

(h) Remove, disable, or render inoperative by deceptive means a security, anti-spyware or anti-virus technology installed on the computer without obtaining prior consent from the User.

(i) Install or execute the Software on the computer with the intent of causing a person to use the software in a way that violates any other provision of this section.

(j) Allow any of their Certified Software to be bundled with the Software unit currently engaging in any of the Prohibited Activities listed in this section;



Trusted Download Program Requirements

(k) Engage in any activity that attempts to defraud consumers, affiliates, merchants, advertisers, or other software publishers. Activities that are specifically prohibited include, but are not limited to:

(i) Shopping cart hijacking; or failing to prevent affiliates or advertisers from using Participant Software to facilitate this activity

(ii) Failing to prevent the Participant Software from facilitating the placement of advertisements, such pop-overs or pop-unders, to gain commission (for the Participant and/or its advertiser and/or affiliate) for traffic that was not originated by the affiliate or the Participant;

(iii) Using forced clicks, redirects, or other deceptive means to generate traffic, downloads, page views or other user activity

(iv) Cookie stuffing: the practice of inserting cookies or similar tracking assets on a User's computer for the purpose of gaining unauthorized commissions for User actions.

(l) Otherwise engage in activities related to these Program Requirements that are fraudulent, misleading, unlawful, or violative of the rights of third parties.

15. Scope of Certification. Material Changes to the Certified Software may trigger a recertification requirement.