I. Scope

TRUSTe has been approved as a recognized privacy certification organization by the 21 member Economies of the Asia Pacific Economic Cooperation (APEC). TRUSTe’s APEC Privacy Certification program is designed to evaluate the privacy policies and practices of businesses collecting or processing personal information against TRUSTe’s APEC Privacy Certification Standards. These Certification Standards are based on the APEC Cross Border Privacy Rules (CBPR)Program Requirements. This program certifies both online and offline data collection practices of businesses as being in compliance with the requirements of the CBPR system. In order to be eligible for APEC certification, businesses must have their primary location in the United States and be subject to the jurisdiction of the Federal Trade Commission.

In order for a business to successfully obtain a TRUSTe APEC Privacy Certification, the business must provide access to its privacy and data governance practices in order to be evaluated against these APEC Privacy Certification Standards (Certification Standards). Upon satisfactory evaluation, TRUSTe offers an APEC Privacy Certification seal and validation page that attests to the business’ CBPR compliance.

Terms defined in Section II of these Certification Standards are bolded the first time they appear in this document.

II. Minimum Certification Standards

A. Any Participant seeking certification that their privacy policies and practices comply with TRUSTe’s APEC Privacy Certification Standards shall demonstrate compliance with the following:

B. Privacy Statement

1. Participant must maintain and abide by an accurate and up-to-date Privacy Statement approved by TRUSTe in its sole discretion. This Privacy Statement must provide information on the Participant's privacy practices including:

   a) A definition of the scope of the Privacy Statement;

   b) Types of Personal Information (PI) collected, either through active or passive means;

   c) The identity of the Participant (e.g. company name) collecting PI;

   d) Types of entity(ies) other than the Participant, excluding Service Providers, collecting PI;

   e) Manner in which collected PI is used. Just-in-Time Notice is required if there is distribution or disclosure for a Primary or Secondary Purpose, excluding Service Providers;

   f) Types of Third Parties, if any, with whom collected PI is shared and for what purpose;

   g) Whether PI is appended with information obtained from third party sources, the types of information being appended, and the purpose for appending collected information;
h) A description of the method for updating privacy settings or exercising choice, including choice for interest-based advertising, as required in these Certification Standards;

i) A description, as required in these Certification Standards, of the method to request access to, or deletion of, collected PI;

j) A statement confirming that any requests for access or deletion will receive a response within a reasonable timeframe;

k) A general description of the Participant’s information retention policies, and the types of information security measures in place to protect collected PI as required in these Certification Standards;

l) Types of passive collection technologies used by the Participant or Third Parties including Service Providers and the purpose for using those technologies (e.g., cookies, web beacons, device recognition technologies);

m) A description of the method for contacting the Participant, including company name, email address or a link to an online form, and physical address;

n) A description of the method for notification of any Material Changes in the Participant’s privacy practices;

o) A statement that collected PI is subject to disclosure pursuant to judicial or other governmental subpoenas, warrants, orders, or goes bankrupt, or to protect the rights of the Participant, or protect the safety of the Individual or the safety of others.

p) The effective date of the Privacy Statement;

q) A statement that Participant complies with the APEC Cross Border Privacy Rules System; and

r) Clear and Conspicuous access to the Validation Page, as outlined in TRUSTe’s guidelines, and how to contact TRUSTe to express concerns regarding Participant’s Privacy Statement or privacy practices.

2. At a minimum, Participant must provide access to a Comprehensive Privacy Statement that discloses the Participant’s information practices.

3. Access to the Privacy Statement must be Clear and Conspicuous and easily accessible.

4. As reasonably practicable, Privacy Statement must be available when the Individual engages with the Participant.

5. Privacy statement must be available when PI is collected, or reasonably soon after in the event if it is not reasonably practicable to provide it at the time of PI collection.
6. Participant must treat all collected information in accordance with the posted Privacy Statement in effect at the time of collection unless the Individual otherwise has given Express Consent as required in Section II.C.3 of these Certification Standards.

7. **Short Notice**

   a) If Participant chooses, they may provide a **Short Notice** highlighting their information practices.

   b) The Short Notice must be Clear and Conspicuous and easily accessible.

   c) Short Notice must link to Comprehensive Privacy Statement.

   d) The Comprehensive Privacy Statement must be Clear and Conspicuous and easily accessible from the Short Notice.

   e) Clear and Conspicuous access to the Validation Page, as outlined in TRUSTe's guidelines, and to information on how to contact TRUSTe to express concerns regarding Participant's Privacy Statement or privacy practices.

   f) Any Short Notice must be consistent with Comprehensive Privacy Statement.

8. **Just in Time Notice**

   a) If Participant chooses to provide Just in Time Notice, the Just in Time Notice must be consistent with the Comprehensive Privacy Statement.

9. **Foreign Language Privacy Statement**

   a) The Privacy Statement must be provided in the same language in which the Participant's business operates.

   b) If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe must use reasonable efforts to verify that Participant's **Foreign Language Privacy Statement** accurately describes the Participant's privacy practices and meets the Participant's obligations under these Certification Standards.

   c) Participant must notify TRUSTe of any Material Changes to its Foreign Language Privacy Statement and submit changes to TRUSTe for review and approval as required in Section II.C.8.c) of these Certification Standards.
C. Privacy Policies and Practices

The following requirements apply if the Participant collects or processes PI:

1. Collection Limitation:

   a) Participant must represent it understands that it has an independent obligation to comply with any law or regulation of the jurisdiction that governs the collection of PI. At all times PI must be collected by lawful and fair means.

   b) Participant may only collect PI where such collection is:

      (1) Limited to information reasonably useful for the purpose for which it was collected, and in accordance with the Participant’s Privacy Statement in effect at the time of collection; or

      (2) With notice to and Express Consent of the Individual.

2. Use of PI

   a) Participant may use PI in the provision of advertised services. Such use(s) must be in accordance with their published Privacy Statement in effect at the time of collection, or with notice to and Express Consent of the Individual.

   b) Information collected by the Participant or the Participant’s Service Provider may be used to tailor the Individual’s experience.

3. Choice

   a) Participant must offer the Individual control over their collected PI as follows:

      (1) Participant must obtain Express Consent prior to sharing PI in any manner not in accordance with their posted Privacy Statement in effect at the time of collection;

      (2) Express Consent must be obtained prior to the sharing of Sensitive Information to Third Parties other than Service Providers;

      (3) Participant must provide an opportunity to withdraw Express Consent previously provided to having PI used by the Participant in any manner not in accordance with their published Privacy Statement in effect at the time of collection;
APEC Privacy Certification Standards

(4) Participant must provide instructions and access to a mechanism that enables the Individual to withdraw consent for the use of their information for the purposes of interest-based advertising;

(5) Participant must honor and maintain the Individual’s choice selection in a persistent manner until such time the Individual changes that choice selection; and

(6) Participant must provide a means by which the Individual may withdraw consent or change their choice selection.

b) Consent is not necessary where the use, disclosure or distribution of PI is required by law, court order, or other valid legal process.

c) The Privacy Statement must state when choice can be exercised over the collection, use, and disclosure of PI and Sensitive Information, and describe how to exercise choice.

d) Such choice mechanism must be Clear and Conspicuous, easy to use and affordable.

4. Collection and Use of Third Party PI

a) Participant must use Third Party PI collected to facilitate the completion of the transaction that is the Primary Purpose for which the information was collected.

b) Participant must obtain Express Consent from the Individual to whom such Third Party PI pertains before such Third Party PI may be used, or disclosed by the Participant for any purpose other than the Primary Purpose for which such PI was collected.

(1) Participant may use Third Party PI to send a one-time email message to the Individual to solicit their Express Consent.

c) Regarding Third Party PI, the Privacy Statement must state:

(1) The types of the entity(ies) collecting Third Party PI;

(2) The types of Third Party PI is collected, either through active or passive means;

(3) The manner in which collected Third Party PI is used and/or disclosed; and

(4) The types of additional Third Parties if any, including Service Providers, with whom collected Third Party PI is shared.
d) A Participant that compiles information about Individuals, who are neither customers nor registered users of that Participant's services and sells access to that information to Third Parties may provide the information, including search results, containing Third Party PI without the notice and choice requirements noted above, provided:

(1) The Information obtained is from public or published sources which have no prohibition around onward transfer or use associated with the information;

(2) The Participant provides a mechanism to stop having information displayed in its search result;

(3) Such mechanism must be easily accessible; and

(4) The Privacy Statement clearly describes how the Individual can stop information from being displayed in its search results.

e) This does not include situations where Participant disclosed Third Party PI back to an entity that has rights to such information.

f) If Participant allows import of Third Party PI, Participant must provide a Clear and Conspicuous and easily accessible notice to the user as to why they are providing a password or other access to their contacts or email account.

5. User Public Profiles

a) Participant must remind the Individual within a reasonable time period after profile creation that they have created a public profile.

b) Participant must provide a reasonable and appropriate mechanism to allow the Individual to manage their privacy settings to control the extent that the Individual’s created profile is publicly displayed. This mechanism must:

(1) Be consistent with how the Individual normally interacts or communicates with the Participant;

(2) Be Clear and Conspicuous, and easy to use; and

(3) Confirm to Individual that privacy settings have been set-

(c) The Privacy Statement must state how the Individual can update their privacy settings.

6. Access

a) Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PI;
APEC Privacy Certification Standards

b) Participant must implement reasonable mechanisms to allow the Individual to request deletion of PI or that collected PI no longer be used;

c) Such mechanism must be consistent with how the Individual normally interacts or communicates with the Participant;

d) Such mechanism or process must be Clear and Conspicuous, and easy to use;

e) Such mechanism or process must confirm to the Individual that any inaccuracies have been corrected.

f) The Participant’s privacy statement must describe how access is provided.

g) The Participant must notify Third Parties if an Individual’s PI transferred to that Third Party has been modified or updated after the transfer.

h) Participant is not required to permit Individual access to PI or delete PI to the extent that:

   (1) Such access or deletion would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant’s confidential information or the confidential information of others;

   (2) The burden or cost of providing access or deletion would be disproportionate or the legitimate rights or interests of others would be violated. However, Participant may not deny access or deletion on the basis of cost if the Individual offers to pay the costs; or

   (3) The requested PI is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information.

i) Participant must have a mechanism for the Individual to request removal from displayed search results if the display of such results will:

   (1) Cause physical harm to the Individual; or

   (2) Interfere with the safeguarding of important countervailing public interests, including national security, defense, or public security.

j) If Participant denies access or deletion to PI, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access.
k) Participant must respond to all access or deletion requests within a reasonable timeframe.

7. Promotional and Newsletter Media Communications

   a) Promotional and newsletter media communications sent by the Participant must include Participant’s postal address and a Clear and Conspicuous functional unsubscribe mechanism.

   b) Participant must honor the Individual’s request to unsubscribe from a promotional or newsletter media communication beginning on the tenth (10) business day after the Participant receives the unsubscribe request, unless the Individual subsequently requests to receive promotional or media communications from the Participant.

   c) An unsubscribe mechanism is not required for administrative or customer service-related messages (e.g., account management or provisioning of requested services, warranty or recall information, safety or security announcements).

8. Material Changes

   a) Participant must notify Individuals of any Material Changes to its privacy practices and/or Privacy Statement prior to making the change;

   b) Privacy Statement must describe the method for providing notification; and

   c) Participant must obtain prior approval from TRUSTe:

      (1) For any Material Change to its Privacy Practices and/or Privacy Statement; and

      (2) For content and method of notice.

D. Data Governance

1. Participant must have processes in place to comply with these Certification Standards.

2. Participant must implement appropriate controls and processes to manage and protect PI within its control including the ones listed in this Section II.D.

3. Such controls and processes must be appropriate to the level of sensitivity of the data collected and stored, and the severity of the harm threatened.
4. Data Security

a) Participant must implement reasonable policies and procedures to protect PI within its control from unauthorized access, use, alteration, disclosure, or distribution.

b) Participant must maintain and audit internal information technology systems within Participant's control such as:

   (1) Authentication and access controls;

   (2) Boundary protections measures (e.g., firewalls, intrusion detection);

   (3) Regularly monitor and repair systems including servers and desktops for known vulnerabilities;

   (4) Limit access and use of PI, or Third Party PI, to Personnel with a legitimate business need where inappropriate access, use, or disclosure of such PI, or Third Party PI, could cause financial, physical, or reputational harm to the Individual;

   (5) Implement protection against phishing, spam, viruses, data loss, and malware;

   (6) Implement processes for the secure disposal of PI, and;

   (7) Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.

c) At a minimum, access to PI or Third Party PI retained by Participant must be restricted by username and password.

d) The Privacy Statement must state that security measures are in place to protect collected PI and/or Third Party PI.

5. Data Quality and Integrity

a) Participant must take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PI to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.

b) If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant must promptly delete or modify that item of information, as appropriate, based on the results of the investigation.
6. Data Retention

a) If a Participant receives and retains PI or Third Party PI, the Participant shall limit its retention to no longer than reasonably useful to carry out its legitimate business purpose, or legally required; and must disclose this in the Privacy Statement.

b) Regardless of the time period of retention, so long as a Participant has PI or Third Party PI in its possession or control, the requirements included herein must apply to such information.

7. Third Party Data Sources

a) All data sources that the Participant uses must contain appropriate terms of use showing that all data received was obtained under legitimate means and that limitations regarding the collection, use, and onward transfer of the PI are satisfied.

8. Service Providers

a) Participant must take reasonable steps to ensure that its Service Providers that collect, process, or distribute PI on the Participant’s behalf either:

   (1) Abide by privacy and security policies that are substantially equivalent to Participant’s policies; or

   (2) Abide by the rights and obligations attached to the PI by the Participant as stated in the Privacy Statement in effect at the time of collection including the security, confidentiality, integrity, use, and disclosure of the PI.

b) Participant must take reasonable steps to ensure its Service Providers using Sub-Processors to collect, process, or distribute PI on its behalf are required to abide by the rights and obligations attached to the PI by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PI.

9. Training

a) The Participant must conduct regular training of Personnel regarding:

   (1) Maintaining the security, confidentiality and integrity of PI and Third Party PI it receives from an Individual;

   (2) The Participant’s privacy policies, and information collection, destruction, and use practices; and

   (3) The Participant’s Business Continuity Plan and Disaster Recovery Program.
10. **User Complaints and Feedback**

   a) The Participant must provide users with reasonable, appropriate, timely, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant’s privacy practices.

   b) The Participant must also cooperate with TRUSTe’s efforts to investigate and resolve non-frivolous privacy complaints, questions and concerns raised either by:

      (1) Users through TRUSTe’s dispute resolution process; or

      (2) TRUSTe.

11. **Data Breach**

   a) The Participant shall notify affected Individuals of a known data breach as required by law.

   b) The Participant, if legally required to notify Individuals of a data breach, must notify TRUSTe and provide a copy of the notice to be sent or sent to affected Individual(s).

E. **Participant Accountability**

1. **Cooperation with TRUSTe**

   a) Provide, at no charge to TRUSTe or its representatives, full access to the online properties (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices.

   b) The Participant shall provide, upon TRUSTe's reasonable request, information including copies of all relevant policies regarding how PI is gathered and used.

   c) Cooperation with additional verification activities by TRUSTe as warranted, including periodic compliance monitoring, or third-party onsite audits that are payable by the Participant.

2. **Annual Recertification**

   a) The Participant shall undergo re-certification to verify ongoing compliance with these Certification Standards annually.

3. **Termination for Material Breach**

   a) In the event TRUSTe reasonably believes the Participant has materially breached these Certification Standards, TRUSTe may terminate the Participant's participation in this program upon twenty (20) business days' prior written notice ("Notice of Termination") unless the breach is corrected within the same twenty (20) business day period ("Cure Period").
b) Material breaches of these Certification Standards include but are not limited to:

(1) Participant’s continual, intentional, and material failure to adhere to these Certification Standards;

(2) Participant’s material failure to permit or cooperate with a TRUSTe investigation or review of Participant’s policies or practices pursuant to the Certification Standards;

(3) Participant’s continual, intentional, and material failure to comply with any Suspension Obligations;

(4) Participant’s material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe; or

(5) Any deceptive trade practices by the Participant.

4. Suspension Status

a) In the event TRUSTe reasonably believes that Participant has materially violated these Certification Standards, Participant may be placed on suspension.

b) Notice will be provided of the violation and any remedial actions that TRUSTe will require Participant to take during the Suspension Period (“Suspension Obligations”).

c) Participant will be considered to be on Suspension immediately upon receiving notice from TRUSTe. Suspension shall last until such time as the Participant has corrected the material breach or Certification Standards violation to TRUSTe’s satisfaction, but not for a period of greater than six (6) months (“Suspension Period”) unless mutually agreed by the Parties.

d) Suspension Obligations may include, but are not limited to:

(1) Compliance with additional Certification Standards;

(2) Cooperation with heightened compliance monitoring by TRUSTe and additional verification activities, including third-party onsite audits as warranted; and

(3) Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe’s additional onsite audits and compliance monitoring.

(4) Participant must comply with all Suspension Obligations.
(e) During the Suspension Period, Participant’s status may be indicated via a TRUSTe Validation webpage or TRUSTe may require Participant to cease using the TRUSTe trustmarks.

(f) At the end of the Suspension Period, TRUSTe will, in its discretion, either:

1. Determine that Participant has complied with Participant’s Suspension Obligations, thereby satisfying TRUSTe’s concerns;

2. Extend the Suspension Period by mutual agreement with the Participant; or

3. Determine that Participant has failed to comply with Participant’s Suspension Obligations and immediately terminate Participant for cause.

III. Definitions
The following definitions shall apply herein:

A. “Clear and Conspicuous” means a notice that is reasonably easy to find, and easily understandable in terms of content and style to the average reader.

B. “Express Consent” means the affirmative consent (opt-in) to a practice by the Individual, after being provided notice, but prior to implementing the practice.

C. “Foreign Language Privacy Statement” is the Participant’s Privacy Statement translated into a language other than English.

D. “Individual” means the discrete person to whom the collected information pertains.

E. “Material Change” means degradation in the rights or obligations enumerated in these Certification Standards.

F. "Participant" means the entity that has entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the Certification Standards included therein.

G. “Personal Information (PI)” means any information or combination of information that can be used to identify, contact, or locate a discrete Individual.

H. “Personnel” means all Participant employees, contractors, subcontractors and agents provided access to the Individual’s information for the purpose of inputting, processing, managing, deleting, or securing it.
I. "Primary Purpose" means use of PI that is reasonably expected by the Individual (i) at the point of collection; and (ii) including compatible uses in features and services to the Individual that do not materially change expectations of user control and third party sharing. Such use may be at least those uses described in the Participant's terms of service governing the Participant's products or services which give rise to the Individual's interaction with the Participant.

J. "Privacy Statement" shall mean the statements of Participant's information collection and usage practices, as such practices are updated from time to time. Participant's Privacy Statement includes, but is not limited to:
   1. A single, comprehensive statement of all the Participant's information practices ("Comprehensive Privacy Statement");
   2. A summary notice highlighting the Participant's information practices ("Short Notice"); or
   3. Disclosure of specific information practices posted at the point of information collection ("Just in Time Notice").

K. "Publicly Available Information (PAI)" means any information reasonably believed to be lawfully made available to the general public from:
   1. Federal, state or local government records;
   2. Widely available source(s) having no additional prohibition around onward transfer or use; or
   3. Disclosures to the general public that are required to be made by federal, state or local law.

L. "Secondary Purpose" is the use of PI in a way that is not reasonably expected by the Individual relative to the transactions or ongoing services provided to the Individual by Participant or the Participant's Service Provider. Such purpose may or may not be described by Participant's terms of service governing Participant's products or services which give rise to the Individual's interaction with the Participant.

M. "Sensitive Information" is information where unauthorized use or disclosure of that information would reasonably or foreseeably likely to cause financial, physical, discriminatory or reputational harm to an Individual. Examples of Sensitive Information may include:
   1. Financial Information such as credit card or bank account number;
   2. Government-issued identifiers such as SSN, driver's license number;
   3. Insurance plan numbers;
   4. Racial or ethnic origin of the Individual;
   5. Political opinions of the Individual;
   6. Religious, philosophical, or similar beliefs of the Individual;
   7. Individual's trade union membership;
8. Precise information regarding the Individual’s past, present, or future physical or mental health condition and treatments including genetic, genomic, and family medical history;
9. Individual’s sexual life or orientation;
10. Individual’s real-time geo-location or historical precise geo-location information;
11. The commission or alleged commission of any offense by the Individual; or
12. Any proceedings for any committed or allegedly committed offense by the Individual and the disposal of such proceedings or the sentence of any court in such proceedings.

N. “Service Provider” is anyone other than the Participant or the Individual that performs, or assists in the performance of, a function or activity which may involve the use or disclosure of PI or Third Party PI. Such use shall only be on behalf of Participant or Individual and only for the purpose of performing or assisting in that specific function or activity as agreed to by the Participant and Individual.

O. “Sub-Processor(s)” is a Third Party that has contractually agreed to provide services such as data input, data processing, deletion, and data storage on behalf of a Service Provider in accordance with the instructions of the Participant.

P. “Third Party(ies)” is an entity(ies) other than the Participant or the Individual which is not directly affiliated with the Participant; and, if affiliated with the Participant, where such affiliation is not reasonably known to the Individual.

Q. “Third Party Personal Information (Third Party PI)” means PI that is collected by Participant from an entity other than the Individual.

R. “Validation Page” is a webpage controlled and hosted by TRUSTe that verifies the Participant’s certification status, and the TRUSTe certification scope.