I. Program Description
TRUSTe’s Enterprise Privacy Certification Standards (Certification Standards) apply to businesses who collect or process personal information, and set a standard for responsible data collection practices. These Certification Standards are based on foundational privacy frameworks including the Fair Information Practice Principles, OECD Privacy Guidelines, APEC Privacy Framework, and the EU-U.S. and Swiss-U.S. Privacy Shield Principles. This program offers businesses the ability to certify its online data collection practices (option to extend to offline practices) as being in compliance with TRUSTe’s Enterprise Privacy Certification Standards, thus providing businesses the flexibility to broadly or narrowly define the certification scope to meet strategic business and privacy goals.

In order for a business to successfully obtain a TRUSTe Enterprise Privacy Certification, the business must provide access to its privacy and data governance practices to be evaluated against these Certification Standards. Upon satisfactory evaluation, TRUSTe offers a privacy certification seal and Validation Page that attests to the business’s compliance with these Certification Standards.

Defined terms appearing in Section II of these Certification Standards are bolded the first time they appear in this document.

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

A. Privacy Notice

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

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

   b) Types of Personal Information (PI) or Third-Party PI collected, either directly through active or passive means, or received from third-party sources (e.g., data append);
Enterprise Privacy Certification Standards

c) The identity of the Participant (e.g., company name), and, where applicable, the identity of subsidiaries collecting PI or Third-Party PI;

d) Types of entity(ies) other than the Participant, including **Service Providers**, collecting PI or Third-Party PI;

e) Purpose(s) for which collected PI or Third-Party PI is used;

f) Types of **Third Parties**, if any, with whom collected PI or Third-Party PI is shared and for what purpose(s);


g) A description of the method for updating privacy settings or exercising choice, including choice for interest-based advertising, as required in these Certification Standards;

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

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

j) 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);

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

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

m) A statement that collected PI or Third-Party PI is subject to disclosure pursuant to judicial or other governmental subpoenas, warrants, orders, or other lawful requests by public authorities; in the event that Participant files for bankruptcy; to protect the rights of the Participant; or protect the safety of the **Individual** or others.

n) The effective date of the Privacy Notice; and
Enterprise Privacy Certification Standards

2. Participant must provide access to a single comprehensive Privacy Notice.

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

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

5. Privacy Notice must be available when PI or Third-Party PI is collected, or reasonably soon after in the event it is not reasonably practicable to provide it at the time of collection.

6. The Privacy Notice must be provided prior to the Participant using collected PI for a purpose other than that for which it was originally collected or disclosing it for the first time to a Third Party.

7. Participant must treat all collected information in accordance with the posted Privacy Notice in effect at the time of collection unless the Individual has otherwise given Express Consent as required in Section II.B.3 of these Certification Standards.

8. If the Participant wants to self-certify with the U.S. Department of Commerce for compliance with either the EU-U.S. or Swiss-U.S. Privacy Shield Principles (Principles) the Participant’s Privacy Notice must also include information about:

   a) Its participation in EU-U.S and/or Swiss-U.S.. Privacy Shield and a link to or web address for the EU-U.S and/or Swiss-U.S.. Privacy Shield list;

   b) Participant’s commitment to apply the Principles to all PI received from the EU in reliance on the EU-U.S. Privacy Shield and/or PI received from Switzerland in reliance on the Swiss-U.S. Privacy Shield;

   c) The entities or subsidiaries of the Participant’s organization that are also adhering to the Principles;
d) The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the Individual.

(1) EU: Participant must identify whether this dispute resolution body is: (1) the panel established by European Data Protection Authorities, (2) an alternative dispute resolution (ADR) provider based in the EU, or (3) an ADR provider based in the United States; and/or

(2) Swiss: Participant must identify whether this dispute resolution body is: (1) the Commissioner, (2) an alternative dispute resolution (ADR) provider based in Switzerland, or (3) an ADR provider based in the United States.

e) Being subject to the investigatory and enforcement powers of the Federal Trade Commission, the U.S. Department of Transportation or any other U.S. authorized statutory body;

f) The possibility, under certain conditions, for the Individual to invoke binding arbitration;

g) Its liability in cases of onward transfer to Third Parties; and

h) Any relevant establishment based in the EU and/or Switzerland that can respond to Individuals’ inquiries or complaints, along with contact information for that establishment.

9. Foreign Language Privacy Notice

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

b) If Participant seeks TRUSTe certification of a Privacy Notice in a language other than English, TRUSTe will use reasonable efforts to verify that Participant’s Foreign Language Privacy Notice 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 Notice and submit changes to TRUSTe for review and approval as required in Section II.B.7.c) of these Certification Standards.
B. Privacy Policies and Practices

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 or Third-Party PI. At all times, PI and Third-Party PI must be collected by lawful and fair means.
   
b) Participant may only collect PI or Third-Party PI where such collection is:

   (1) Limited to information relevant for the purpose for which it was collected, and in accordance with the Participant’s Privacy Notice 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 Notice 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(s) 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 Notice 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 or 
disclosed by the Participant in any manner not in 
accordance with their published Privacy Notice in effect at 
the time of collection;

(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 Notice must state when choice can be exercised 
over the collection, use, and disclosure of PI and Sensitive 
Information, and describe how Individuals may exercise choice.

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

4. Use of Third-Party PI

a) Participant may use collected Third-Party PI 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) 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 is easily accessible; and

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

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

e) 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. **Access**

a) Participant must implement reasonable and appropriate mechanisms to allow the Individual to determine whether the Participant holds or is processing information related to the Individual, and to correct or update inaccurate or incomplete PI.

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) PI must be provided to the Individual in an understandable format.

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 to access 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) Such access or deletion interferes with the execution or enforcement of the law or with private causes of action, including the prevention, investigation, or detection of offenses or the right to a fair trial;

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

(4) 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.

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.

6. Promotional and Newsletter Media Communications
Enterprise Privacy Certification Standards

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).

7. Material Changes

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

b) Privacy Notice 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 Notice; and

(2) For content and method of notice.

C. 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 or Third-Party PI within its control, including those listed in this Section II.C.

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 and Third-Party PII within its control from unauthorized access, use, alteration, disclosure, or distribution.

   b) Participant must maintain and audit the internal information technology systems within its 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 and 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 deletion, return, or secure disposal of PI or Third-Party PII; 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 PII retained by Participant must be restricted by username and password.

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

5. **Data Quality and Integrity**
Enterprise Privacy Certification Standards

a) Participant must take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PI or Third-Party 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 the 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 is necessary for uses that are not incompatible to the purpose of collection.

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. Transfers to Third Parties

a) If Participant transfers or otherwise discloses PI to a Third Party not acting as a Service Provider, the Participant must:

(1) Enter into a contract with that Third Party requiring that PI may be processed for limited and specified purposes consistent with the consent provided by the Individual;

(2) Ensure that the Third Party will abide by the rights and obligations attached to the PI by the Participant as stated in the Privacy Notice in effect at the time of collection including the security, confidentiality, integrity, use, and disclosure of the PI; and

(3) Require the Third Party to notify the Participant if the Third Party determines it is no longer able to abide by the rights and obligations attached to the PI, and to cease using that PI or otherwise take appropriate steps to remediate.
b) A contract may not be required if data is transferred between a controlled group of companies and other mechanisms such as EU Binding Corporate Rules or other intra-group mechanisms are in place ensuring the continuity of protection of personal information.

c) If Participant transfers PI, or otherwise discloses or makes available PI or Third-Party PI to Service Providers, the Participant must take reasonable steps to ensure the following:

(1) Transfers of PI or Third-Party PI to Service Providers must be for limited and specified purposes, and be specified in the contract or service agreement.

(2) Participant must take reasonable steps to require and ensure that its contracted Service Providers that collect, process, or distribute PI or Third-Party PI on the Participant’s behalf:

   (i) Act only on the instructions of the Participant;

   (ii) Provide appropriate technical and organizational measures to protect PI or Third-Party PI from accidental or unlawful destruction, accidental loss or alteration, and unauthorized disclosure or access;

   (iii) Understand whether onward transfer is allowed; and

   (iv) If the Service Provider determines it is no longer able to abide by the rights and obligations attached to the PI or Third-Party PI, it must:

       1. Notify the Participant,
       2. Cease using that PI or Third-Party PI, and
       3. Take appropriate steps to remediate.

   (iv) Assist the Participant, when appropriate, in responding to Individuals exercising their rights to notice, choice, access, and privacy-related complaint resolution; and
Enterprise Privacy Certification Standards

(v) Require its Sub-Processors that collect, process, or distribute PI or Third-Party PI to abide by the rights and obligations attached to the PI or Third-Party PI by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PI or Third-Party PI.

(3) Participant, upon learning of unauthorized use of PI or Third-Party PI by its contracted Service Providers, must take appropriate and reasonable steps to stop and remediate any unauthorized use of PI or Third-Party PI.

d) Participant must comply with any law or regulation of the jurisdiction that governs the disclosure or transfer of PI or Third-Party PI to Third Parties.

8. 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.

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.

b) Training should be appropriate to Personnel’s role and job function.

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 respond to the individual in a timely manner, not to exceed 45 days, upon receiving a complaint, concern, or feedback directly from an individual regarding the Participant’s privacy practices.

c) The Participant must also cooperate with TRUSTe’s efforts to investigate and resolve non-frivolous privacy-related 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).

D. Participant Accountability

1. Cooperation with TRUSTe

   a) Participant shall provide, at no charge to TRUSTe or its representatives, full access to the online properties (e.g., including password access to premium or members-only areas) for the purpose of conducting reviews to ensure that Participant’s Privacy Notice(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.
Enterprise Privacy Certification Standards

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 Review**

   a) The Participant shall undergo an **Annual Review** to verify ongoing compliance with these Certification Standards.

   b) If issues of non-compliance with any of these Certification Standards are found as a result, TRUSTe will investigate the compliance issue, notify the Participant, outline the corrections necessary and provide a reasonable timeframe for the Participant to make such changes, during which time, TRUSTe will work with the Participant to ensure the necessary changes are made.

   c) TRUSTe will discontinue the Participant’s certification if the Participant fails to correct required changes within a reasonable timeframe as determined by TRUSTe.

3. **Certification Status**

   a) In the event TRUSTe determines that Participant’s compliance with these Certification Standards has lapsed, TRUSTe will provide notice, and if not resolved within a reasonable timeframe as determined by TRUSTe, discontinue Participant’s certification.

      (1) TRUSTe may reinstate the Participant’s certification if the Participant makes all the required changes.

   b) Upon notice to the Participant, TRUSTe may discontinue immediately the Participant’s certification if Participant is found in Material Breach of these Certification Standards. 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 material failure to cooperate with TRUSTe regarding an audit, privacy-related complaint, or the compliance monitoring activities of TRUSTe; or
(4) Any deceptive trade practices by the Participant.
III. Definitions
The following definitions shall apply herein:

A. “Annual Review” is a process to check the Participant’s compliance with these Certification Standards. This process may continue past the anniversary of the prior re-certification date not to exceed a reasonable timeframe as determined by TRUSTe.

B. “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.

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

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

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

F. "Material Change" means degradation in the rights or obligations enumerated in these Certification Standards.

G. “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.

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

I. “Personnel” means all Participant employees, contractors, sub-contractors, and agents provided access to the Individual’s information for the purpose of inputting, processing, managing, deleting, or securing it.
J. "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.

K. "Privacy Notice" shall mean the notices, including a single, comprehensive notice, of the Participant's information collection and usage practices, as such practices are updated from time to time.

L. “Publicly Available Information” 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.

M. "Sensitive Information" is information where unauthorized use or disclosure of that information would be reasonably or foreseeably likely to cause financial, physical, discriminatory, or reputational harm to an Individual. Examples of Sensitive Information include:

1. Financial information such as credit card or bank account number;
2. Government-issued identifiers such as Social Security number, 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 or activities of the Individual;
7. Individual's trade union membership or activities;
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. Information regarding the 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;
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; or
13. Information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending 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” 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” is an entity other than the Participant or the Individual which is not directly affiliated with the Participant; or, 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 web page controlled and hosted by TRUSTe that verifies the Participant’s certification status, and the TRUSTe certification scope.