Assurance Program Governance Standards

Revised on: October 20, 2023

I. Overview

TrustArc Inc ("TrustArc"), under the TRUSTe brand, offers a set of privacy assurance programs that enable organizations to demonstrate responsible data collection and processing practices consistent with regulatory expectations and standards for privacy accountability. These programs are based on the TrustArc Privacy & Data Governance ("P&DG") Framework and/or external regulatory standards such as APEC Cross Border Privacy Rules System, APEC Privacy Rules for Processors, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, and the EU General Data Protection Regulation.

The TRUSTe assurance programs enable an organization to certify or verify its privacy and data governance practices and demonstrate compliance with the TrustArc P&DG Framework and/or external standards by meeting requirements set forth in the program's Assessment Criteria which have been mapped to external frameworks, standards, and regulations. Assurance programs and their corresponding Assessment Criteria are designed to provide organizations the flexibility to broadly or narrowly define the certification scope to meet their strategic business, privacy and data protection goals.

For assurance programs, whether in the form of certification or verification, to be meaningful and effective, TrustArc, the certification body, has put in place program governance that includes robust mechanisms to

- Review and enable organizational demonstration of compliance with the Assessment Criteria;
- Enable individuals to express concerns about a participating company's compliance with the Assessment Criteria; and
- Address a participating company's non-compliance with Assessment Criteria including revocation of the company's certification, verification and any associated seals.

This document outlines the policies, rules, and guidelines (collectively the "Standards") by which TrustArc manages its assurance programs and holds participating organizations accountable for compliance with the Assessment Criteria of the program(s) the organization chooses to participate in. TrustArc may amend these Standards from time to time, and any amendments to these Standards will be published at https://www.trustarc.com/privacy-certification-standards/ and communicated to existing Participants in accordance with the terms of the agreement between TrustArc and the Participant. Participants' obligations to comply with amendments to these Standards and TrustArc's right to enforce these Standards are set forth in the agreement between TrustArc and the Participant.

Organizations participating in any or all of the assurance programs listed below agree to follow the requirements outlined herein:

- Enterprise Privacy & Data Governance Practices Certification
- APEC Cross Border Privacy Rules (“CBPR”) Certification
- APEC Privacy Rules for Processors (“PRP”) Certification
- TRUSTe Data Privacy Framework Verification
- TRUSTe Data Collection Certification

Defined terms appear in **bold**.

II. Assurance Program Policies, Rules, and Guidelines
Any **Participant** seeking TRUSTe certification or verification against TRUSTe's Assessment Criteria for the assurance programs listed in Section I shall also comply with the following:

A. Validation Page

1. **Participant** must provide **Clear and Conspicuous** access to the **Validation Page**, as outlined in TRUSTe's seal usage guidelines, and provide notice of how to contact TrustArc to express concerns regarding **Participant's Privacy Notice** or privacy practices.

2. **Participan**t will only associate with the **Validation Page** the online properties that have been reviewed by TrustArc.

3. The **Validation Page** will describe the scope of the TRUSTe certification or verification aligning with attestations made by the **Participant** regarding certification or verification review scope in the **Participant's Assessment Questionnaire**.

B. Material Changes

1. **Participan**t must notify **Individuals** of any **Material Changes** to its privacy practices and/or **Privacy Notice** prior to making the change;

2. If a **Privacy Notice** is required, i**t** must describe the method for providing notification; and

3. **Participan**t must obtain prior approval from TrustArc:

    a. For any **Material Change** to its data privacy and governance practices and/or **Privacy Notice**; and

    b. For content and method of notice to individuals of such changes.

C. Use of TRUSTe Seal

1. The TRUSTe seal may be displayed on a **Privacy Notice** that has been approved by TrustArc.

2. A **Participant** may only display the TRUSTe seal on online properties that are within the scope of that company's Assurance Program(s) and practices that have been certified or verified by TrustArc.

3. If the seal is displayed on a **Foreign Language Privacy Notice**, the **Participant** will attest that there are no material differences between the practices described in the **Foreign Language Privacy Notice** and practices described in the English language version of the notice reviewed and approved by TrustArc and meets **Participant's** obligations under the Assessment Criteria of the program(s) the **Participant** is participating in.

4. Any TRUSTe seal must be hosted and served by TrustArc. **Participants** may not change or alter the TRUSTe seal in any way, and may only display the TRUSTe seal in the manner expressly instructed by TrustArc.

D. Independent Obligation to Comply with Applicable Laws and Regulations

1. **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, use, disclosure, protection or other processing of **Personal Information (PI)** . At all times, **PI** must be collected by lawful, fair and ethical means.

DI. Controls & Processes

1. **Participant** must have and maintain demonstrable processes in place to comply with the Assessment Criteria of the program(s) they are participating in.

2. **Participant** must implement appropriate controls and processes to manage and protect **PI** within its control, including those listed in the Assessment Criteria of the program(s) they are participating in.

3. Such controls and processes must be appropriate to the level of sensitivity of the data collected, used, stored and disclosed, and the risk of the harm (both likelihood and severity) threatened.

DII. TRUSTe Privacy Feedback and Dispute Resolution Mechanism

1. The **Participant** must participate in the TRUSTe Privacy Feedback & Dispute Resolution process, and cooperate with TrustArc's efforts to investigate and resolve non-frivolous privacy-related complaints, questions, and concerns raised either by:

a. Users through TRUSTe's Privacy Feedback and Dispute Resolution process; or

b. TrustArc through its independent monitoring checks.

G. Data Breach

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

H. Participation in Multiple Assurance Programs

I. For **Participants** certified or verified under more than one Assurance Program TrustArc will:
   a. Assess the **Participant** against the Assessment Criteria for all programs the **Participant** is participating in; and
   b. If the Assessment Criteria for one program has a higher standard (e.g., express consent versus opt-out; more prescriptive third party contracting or due diligence standards; more stringent security controls) TrustArc will apply the higher standard unless: (1) the scope of participation in one Assurance Program versus the other is clearly defined and transparently communicated by the **Participant**, and (2) and the **Participant** has separate **Privacy Notices** applicable to the activities within the scope of each Assurance Program in which it participates, and (3) and the **Participant** displays only the applicable seal on the **Privacy Notice** approved under that Assurance Program.

J. Cooperation with TrustArc to Verify Privacy Practices

1. **Participant** shall provide upon TrustArc's reasonable request and at no charge to TrustArc 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 checks to ensure that **Participant's** privacy practices meet the program's Assessment Criteria and **Privacy Notice(s**) is consistent with actual practices.

2. The **Participant** shall provide, upon TrustArc's reasonable request, information including copies of all relevant policies, procedures or descriptions of any processes, or other documentation regarding how **PI** is obtained, collected, used, transferred or disseminated to **Processors** or **Third Parties**.

3. Cooperation with additional verification activities by TrustArc as warranted, including periodic compliance monitoring, or onsite audits, including any monitoring or auditing by third parties at the direction of TrustArc, that are payable by the **Participant**. The **Participant** may choose to have TrustArc conduct its certification or verification reviews onsite at the **Participant's** location, costs payable by the **Participant**.

4. TrustArc will conduct random checks of online properties where the TRUSTe seal is hosted to ensure those properties are governed by the policies and practices TrustArc reviewed pursuant to the Participant's Assurance Program(s).

J. Annual Review

1. The **Participant** shall undergo an **Annual Review** to verify ongoing compliance with the Assessment Criteria of the program(s) they are participating in and adherence to these Assurance Program Governance Standards.

2. If issues of non-compliance with any of the Assessment Criteria are found as a result of such **Annual Review**, TrustArc will investigate the compliance issue, notify the **Participan**t, outline the corrections necessary and provide a reasonable timeframe, not to exceed the **Participant**'s anniversary of the prior re-certification date, for the **Participant** to make such changes, during which time, TrustArc will work with the **Participant** to ensure the necessary changes are made.

3. TrustArc will discontinue the **Participant's** certification if the **Participant** fails to provide the necessary information to enable TrustArc to complete the **Annual Review**, to enable timely completion of the **Annual Review**, or to correct required changes by the anniversary of the prior year certification date.

K. Certification Status

1. In the event TrustArc determines that **Participant's** compliance with the Assessment Criteria of the program(s) the **Participant** is participating in has lapsed, TrustArc will provide notice and, if not resolved within a reasonable timeframe as determined by TrustArc, discontinue **Participant's** certification.

2. TrustArc may reinstate the **Participant's** certification if the **Participant** demonstrates to TrustArc, and TrustArc has verified, that all the required changes have been completed.

3. Upon notice to the **Participant**, TrustArc may discontinue immediately the **Participant's** certification if **Participant** is found in material breach of the Assurance Program Governance Standards or Assessment Criteria of the program(s) in which the **Participant** is participating. Material breaches include but are not limited to:

    a. **Participant's** material failure (e.g., unauthorized use of the TrustArc seal, failure to complete **Annual Review** by the anniversary of the prior year certification date) to adhere to the Assessment Criteria of the program(s) in which they are participating;

    b. **Participant's** material failure to permit or cooperate with a TrustArc investigation or review of **Participant's** policies or practices pursuant to the Assurance Program Governance policies, rules, and guidelines;

    c. **Participant's** material failure to cooperate with TrustArc regarding an audit, privacy-related complaint, or the compliance monitoring activities of TrustArc; or

    d. Any deceptive trade practices by the **Participant**.

4. If TrustArc discovers unauthorized use of the TRUSTe seal, TrustArc will notify the **Participant** and discontinue immediately the **Participant's** certification.

III. Definitions
The following definitions shall apply herein:

A. “Annual Review” is a process to check the **Participant**’s compliance with the Assessment Criteria of the program(s) the **Participant** participates in. This process must be completed by the anniversary of the prior year certification date.

B. “Assessment Questionnaire” is a questionnaire completed by the **Participant** regarding their data protection and privacy practices or privacy program. TRUSTe relies on the responses and evidence provided in the questionnaire as part of its certification or verification determination.

C. “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.

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 this Assurance Program Governance document and Assessment Criteria of the program(s) the **Participant** is participating in.

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 this Assurance Program Governance document and Assessment Criteria of the program(s) in which the **Participant** is participating.

H. "Personal Information” (“PI”) means any information about an identified or identifiable **Individual**, including indirect identification of an **Individual** through an identifier (e.g., identification number, location data,online identifier) or through other factors (e.g., genetic, physical, or social identity).

I. "Privacy Notice" shall mean the notices, including a single, comprehensive notice, of the Participant's information collection, use, disclosure and associated data processing practices, as such practices are updated from time to time.

J. “Processor” is an entity processes data on behalf of another entity that performs or assists in the performance of a function or activity which may involve the use or disclosure of **PI**. Such use shall only be on behalf of that entity and only for the purpose of performing or assisting in that specific function or activity as agreed to by the contracting entity. Processors are also known as agents, business associates, service providers, or vendors.

K. “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.

L. “Validation Page” is a web page controlled and hosted by TRUSTe that verifies the **Participant**’s certification status, and the TRUSTe certification scope.