Enterprise Privacy & Data Governance Practices Certification Assessment Criteria

I. INTRODUCTION **2**

II. ASSESSMENT CRITERIA **4**

DATA NECESSITY 4

USE, RETENTION, AND DISPOSAL 6

DISCLOSURE TO THIRD PARTIES AND ONWARD TRANSFER 10

CHOICE AND CONSENT 13

ACCESS AND INDIVIDUAL RIGHTS 19

DATA INTEGRITY AND QUALITY 25

SECURITY 26

TRANSPARENCY 29

AWARENESS AND TRAINING 33

MONITORING AND ASSURANCE 35

III. DEFINITIONS **36**

I. INTRODUCTION

TrustArc Inc ("TrustArc"), under the TRUSTe brand, offers a set of privacy assurance programs that enable organizations that collect or process personal information to demonstrate responsible data collection and processing practices consistent with regulatory expectations and external standards for privacy accountability. The programs are developed using the standards outlined in the TrustArc Privacy & Data Governance ("P&DG") Framework ("Framework"), which are based upon recognized laws and regulatory standards, such as the OECD Privacy Guidelines, the APEC Privacy Framework, the EU General Data Protection Regulation ("GDPR"). the U.S. Health Insurance Portability and Accountability Act ("HIPAA"), ISO 27001 International Standard for Information Security Management Systems. and other privacy laws and regulations globally.

The TRUSTe Enterprise Privacy & Data Governance Practices Certification is designed to enable organizations, in preparation to assess and obtain certification from TRUSTe, to demonstrate that their privacy and data governance practices for personal information comply with the standards outlined in the Framework. The TrustArc P&DG Framework consists of a set of operational controls that is aligned with key privacy laws, regulatory frameworks, and requirements for ethics and compliance programs and information governance programs that supports all 3 phases, BUILD, IMPLEMENT, and DEMONSTRATE, of program management on an ongoing basis. The assessment criteria set forth in this document are aligned with the Standards set forth in the Framework which enable organizations to design and/or engineer effective privacy and data governance controls into organizational processes products and technologies and maintain or enhance those controls throughout the lifecycle for the product, process or technology

The Assessment Criteria are organized by ten of TrustArc's P&DG Framework BUILD, IMPLEMENT, and DEMONSTRATE Standards of:

- Data Necessity
- Use, Retention, and Disposal
- Disclosure to Third Parties and Onward Transfer
- Choice and Consent
- Access and Individual Rights
- Data Integrity and Quality
- Security
- Transparency
- Awareness and Training
- Monitoring and Assurance

Each section contains the Assessment Criteria TRUSTe uses to assess an organization's compliance with the P&DG Framework Standard. Mapping of the Assessment Criteria to the TrustArc Framework standards and controls and external regulatory standards are noted next to the Assessment Criteria.

Any organization participating in a TRUSTe Assurance Program agrees to comply with TRUSTe's Assurance Program Governance Standards, which apply to all TRUSTe Assurance Programs, and the Assessment Criteria of any Program in which the organization chooses to participate. The Assurance Program Governance Standards ensure that the Program is meaningful and effective in its implementation of robust mechanisms to:

- review and enable organizational demonstration of compliance with the Assessment Criteria;
- enable individuals to raise 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 or verification, and any associated seals.

Upon successful completion of the TRUSTe assessment and certification processes, organizations participating in this Program will be issued and authorized to display the TRUSTe Certified Privacy seal.

Defined terms appear in **bold.**

II. ASSESSMENT CRITERIA

DATA NECESSITY Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and coding to mitigate data storage-related risks.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria4**
TrustArc P&DG Standard: *Data Necessity:* Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and coding to mitigate data storage-related risks. **TrustArc P&DG Control** 2.1: Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and	**1. Collection Limitation** Requirement: The **Participant** must limit the **Personal** I**nformation** collected (whether directly or through the use of T**hird Parties** acting on its behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes. Where the **Participant** indicates it only collects **Personal Information** that is relevant to the identified collection purpose or other compatible or related purposes, TRUSTe must require the **Participant** to identify: ● each type of data collected; ● the corresponding stated purpose of collection for each; ● all uses that apply to each type of data; and ● include an explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. Evaluation: Using the above, TRUSTe will verify that the **Participant** limits the amount and type of **Personal Information** collected to that which is relevant to fulfill the stated purposes. Gaps and Remediation: If the **Participant** indicates it does not limit the amount of **Personal Information** collected to what is relevant to the identified collection purpose, TRUSTe must inform

coding to mitigate data storage-related risks. Data Privacy Framework Principles: II.5.a APEC CBPR Requirement: 6 TRUSTe Data Privacy Framework Assessment Criteria 33 GDPR Article 5(1)(c)	the **Participant** that it must limit the use of collected **Personal Information** to those uses that are relevant to fulfilling the purpose(s) for which it is collected and require the **Participant** to identify: ● each type of data collected; ● the corresponding stated purpose of collection for each; ● all uses that apply to each type of data; and ● include an explanation of the compatibility or relatedness of each identified use with the stated purpose of collection.
TrustArc P&DG Standard: *Data Necessity:* Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and coding to mitigate data storage-related risks. **TrustArc P&DG Control** 2.1: Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and	**2. Data Anonymization** Requirement: The **Participant** must leverage anonymization, de-identification, pseudonymization, coding, or similar mechanisms to mitigate data storage-related risks. Evaluation: Where the **Participant** indicates data does not need to be retained as required in Assessment Criteria 6, or no longer needs to be retained in an identifiable form, TRUSTe will verify the **Participant** has processes in place to mitigate data storage-related risks through leveraging anonymization, de-identification, pseudonymization, coding, or similar mechanisms. Gaps and Remediation: If the **Participant** indicates it does not leverage anonymization, de-identification, pseudonymization, and/or coding techniques to mitigate data storage-related risks, then TRUSTe must inform the **Participant** that it must leverage anonymization, de-identification, pseudonymization, coding, or similar mechanisms to mitigate data storage-related risks for data that does not need to be retained or no longer needs to be retained in an identifiable form.

coding to mitigate data storage-related risks.	

USE, RETENTION, AND DISPOSAL Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Use, Retention, and Disposal:* Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected. **TrustArc P&DG Control** 2.2: Ensure data is used solely for purposes that are relevant to and compatible with the purposes for which it was collected. Data Privacy Framework Principles: II.5.a	**3. Purpose Limitation** Requirement: The **Participant** must limit the use of the **Personal Information** it collects (whether directly or through the use of **Third Parties** acting on its behalf) as identified in the **Participant's Privacy Notice** and/or in another demonstrable form of notice provided at the time of collection, to those purposes for which the information was collected, or for other compatible or related purposes. Depending on the circumstances, examples of compatible processing purposes may include purposes to reasonably: • manage customer relations; • fulfill compliance and legal considerations; • conduct audits, and for security and fraud prevention; • preserve or defend the organization's legal rights; or • for other purposes consistent with the expectations of a reasonable person given the context of the collection. Evaluation: TRUSTe must verify the existence of policies and procedures to ensure that all covered **Personal Information** (collected either directly or indirectly through the use of **Third Parties)** is collected in accordance with the purposes identified in the **Participant's Privacy**

APEC CBPR Requirement: 8 TRUSTe Data Privacy Framework Assessment Criteria 32 GDPR Articles 5(1)(a)-(b) and 6(4)	**Notice(s),** and/or in another demonstrable form of the notice provided at the time of collection, in effect at the time of collection or for other compatible or related purposes. Gaps and Remediation: If the **Participant** does not limit the use of the **Personal Information** it collects to those purposes identified in the **Privacy Notice,** and/or in another demonstrable form of the notice provided at the time of collection or for other compatible or related purposes, TRUSTe must consider other circumstances under which the **Participant** collects and uses **Personal Information**.
TrustArc P&DG Standard: *Use, Retention, and Disposal:* Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected. **TrustArc P&DG Control** *2.3:* Keep data in identifiable form only as long as necessary for identified processing purposes of which individuals have been informed. If data are needed for a longer period of time for research- or optimization-related purposes, implement coding, pseudonymization, or similar mechanisms to limit the risk to individuals.	**4. Data *Retention*** Requirement: The **Participant** must only keep data in an identifiable form (e.g., a form that allows for the identification or re-identification of an **Individual**) for only as long as necessary for the processing purposes **Individuals** have been notified of and for which there is a lawful basis for the data processing. If data are needed for longer periods of time (e.g., research or optimization-related purposes), the **Participant** must implement coding, pseudonymization, or similar mechanisms to limit the risk to **Individuals**. Evaluation: TRUSTe must verify that the Participant: ● only keeps data in an identifiable form for only for only as long as necessary for the processing purposes **Individuals** have been notified of and for which there is a lawful basis for the data processing; and ● has implemented coding, pseudonymization, or similar mechanisms to limit the risk to **Individuals** if data are needed for longer periods of time (e.g., research or optimization-related purposes). Gaps and Remediation: If the **Participant** keeps data in an identifiable form for a period longer than necessary for the processing purposes **Individuals** were notified of and for which there is a lawful basis for the data processing or has not implemented coding, pseudonymization, or similar mechanisms to limit the risk to **Individuals** for data needed for longer periods of time, TRUSTe must inform the **Participant** that it:

GDPR Article 5(1)(e)	• must only keep data in an identifiable form for only as long as necessary for the processing purpose; or • implement coding, pseudonymization, or similar mechanisms to limit the risk to **Individuals.**
TrustArc P&DG Standard: *Use, Retention, and Disposal:* Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected. **TrustArc P&DG Control** *2.4:* Ensure that all data processing is legally permissible, including any data disclosures to third parties. Data Privacy Framework Principles: III.8.a.i.2 APEC CBPR Requirement: 7 TRUSTe Data Privacy Framework Assessment Criteria 31 GDPR Articles 5(1)(a) and 6(1)	**5. Lawfulness of Processing** Requirement: The **Participant** must process collected **Personal Information** (whether directly or through the use of **Third Parties** acting on its behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such **Personal Information.** Examples of lawful means include, but are not limited to: consent, a contract with the individual, legal obligation, health and safety of the individual, public interest, legitimate interests as further defined in applicable laws. Evaluation: TRUSTe must require the **Participant** to certify that it is aware of and is complying with the requirements of the jurisdiction that governs the collection and processing of such **Personal Information** and that it is processing information by lawful and fair means, without deception. Gaps and Remediation: If the **Participant** is unable to certify this, TRUSTe must inform the **Participant** that mechanisms to ensure that data processing is lawful and fair are required for compliance with this requirement.

TrustArc P&DG Standard: *Use, Retention, and Disposal:* Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected. **TrustArc P&DG Control** *2.5:* Define and communicate retention periods for personal data used by the process or technology. Data Privacy Framework Principles: II.5.b TRUSTe Data Privacy Framework Assessment Criteria 35 GDPR Articles 5(1)(e), 13-14, and 30(1)(f)	**6. Define and Communicate Retention Periods** Requirement: The **Participant** must define and communicate retention periods for retaining Personal Information (e.g., information retention policy, retention schedules, or retention requirements). Evaluation: TRUSTe must verify the **Participant** has defined and communicated retention periods. This may be achieved through a retention policy, retention schedules for specific data assets or data processing purposes, or defined retention requirements such as those defined in the **Participant's** privacy policies. Gaps and Remediation: If the **Participant** does not have a define retention periods in place and has not communicated such, TRUSTe must inform the **Participant** that the implementation of defined information retention periods and communication of such is required for compliance with this requirement.

DISCLOSURE TO THIRD PARTIES AND ONWARD TRANSFER Preserve the standards and protections for data when it is transferred to third-party organizations and/or across country borders.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Disclosure to Third Parties and Onward Transfer:* Preserve the standards and protections for data when it is transferred to third-party organizations and/or across country borders. **TrustArc P&DG Control** *2.6:* Assess vendors handling personal data for effective safeguards and controls. Data Privacy Framework Principles: II.3.b.ii TRUSTe Data Privacy Framework Assessment Criteria 27 GDPR Article 28.1 ISO 27001 8.2 Information Security Risk Assessment	**7. Evaluate Processors** Requirement: The **Participant** must have a process to evaluate the privacy and security practices of its **Processors** (e.g., agents, business associates, service providers, or vendors) to ensure the **Processor** has effective safeguards and controls in place that comply with the controls and standards herein and with applicable laws. Evaluation: TRUSTe must verify that the **Participant** has a process in place for evaluating its **Processors** have effective safeguards and controls in place that comply with the controls and standards herein and with applicable laws. Gaps and Remediation: If the **Participant** does not have a process to evaluate its **Processors**, TRUSTe must inform the **Participant** that it must have a process to ascertain whether its **Processors** have effective safeguards and controls in place that comply with the controls and standards herein and with applicable laws.

TrustArc P&DG Standard: *Disclosure to Third Parties and Onward Transfer:* Preserve the standards and protections for data when it is transferred to third-party organizations and/or across country borders. **TrustArc P&DG Control** *2.7:* Execute appropriate contracts with vendors supporting the process or technology or with any third parties. APEC CBPR Requirement: 46 GDPR Article 28(3), Article 26, and 5(2) and 24(1)	**8. Contracts with Processors and other Third Parties** Requirement: The **Participant** must have appropriate contracts in place with ● **Processors** (e.g., agents, business associates, service providers, vendors) pertaining to **Personal Information** they process on the Participant's behalf, which limit the processing of Personal Information only in accordance with instructions from the Participant, and which ensures the Participant's obligations to the **Individual** undertaken by the Participant will be met and that appropriate data protections are ● in place; or ● any **Third Party** the **Participant** discloses or otherwise transfers **Personal Information** to. Evaluation: TRUSTe must verify the existence of each type of agreement described. TRUSTe must verify that the **Participant** has entered into a contract with **Processors** or any **Third Party** to ensure data protections appropriate to the nature of the relationship with the **Processor** or **Third Party** are in place. Gaps and Remediation: If the **Participant** does not have appropriate contracts in place, TRUSTe must inform the **Participant** that implementation of a contract with **Processors** or any **Third Party** is required for compliance with this requirement.
TrustArc P&DG Standard: *Disclosure to Third Parties and Onward Transfer:* Preserve the standards and protections for data when it is transferred to third-party organizations and/or across country borders. **TrustArc P&DG Control** *2.8:* Ensure personal data is adequately protected when transferred internationally,	**9. Onward Transfer to Third Parties** Requirement: If the Participant transfers **Personal Information** to a country other than where the **Individual** to whom the **Personal Information** pertains is located, including transfers to **Third Parties**, the **Participant** must ensure transferred data is adequately protected consistent with applicable laws. Evaluation: TRUSTe will verify the **Participant** has adequate protections (e.g., intra-group transfer agreements, agreements with **Processors**) in place when transferring **Personal Information** internationally.

including transfers to third parties and vendors. Data Privacy Framework Principles: II.3.a. APEC CBPR Requirement: 10-13 TRUSTe Data Privacy Framework Assessment Criteria 22 GDPR Articles 44-50 and Article 30(1)(e)	Gaps and Remediation: If the Participant does not have adequation protections in place for international transfers of **Personal Information**, TRUSTe must inform the **Participant** they must put adequate protections in place.

CHOICE AND CONSENT Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individuals to opt-out of ongoing processing.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control** *2.9:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission (consent) where necessary and appropriate, and enable individual to opt out of ongoing processing.	**10. Choice for Use and Disclosure of Personal Information** Requirement: Provide a mechanism for **Individuals** to exercise choice in relation to the use or disclosure of their **Personal Information.** Choice is not required if: ● **Personal Information** is disclosed to a **Processor** (e.g., agent, business associate, service provider, vendor) for the purpose of **Processing** on behalf of the **Participant**; ● **Personal Information** is not used for: ○ an unrelated or incompatible purpose for which it was collected; ○ direct marketing purposes; or ○ purposes not authorized by the **Individual**; ● **Personal information** is collected lawfully for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives; ● **Processing** is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; ● **Personal Information** is obtained by investment bankers and auditors for the purpose of conducting due diligence as part of a merger or acquisition; ● **Personal Information** is available through public sources of information and has been not combined with information from non-public sources or is subject to restrictions; ● The **Participant** collects, uses, retains, sells, or discloses information that is aggregated or de-identified; ● **Personal Information** is disclosed in response to lawful requests by public authorities, including to meet national security or law enforcement requirements;

Data Privacy Framework Principles: II.2.a.i APEC CBPR Requirement: 15 & 16 TRUSTe Data Privacy Framework Assessment Criteria 19	● **Processing** is based on a determination that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the **Participant** who is a **Controller**; or ● The **Participant,** who is a **Controller,** needs to **Process** the data for the establishment, exercise, or defense of legal claims. Evaluation: TRUSTe must verify that the **Participant** provides a description of the mechanisms provided to **Individuals** so that they may exercise choice in relation to the use or disclosure of their **Personal Information**, such as: ● online at point of collection; ● online via a preference/profile page; ● via contact to the **Participant's** privacy office whether online or offline; ● via e-mail to a designated contact within the **Participant** organization; ● via telephone to a designated contact within the **Participant** organization; or ● via postal mail to a designated contact within the **Participant** organization. TRUSTe must verify that these types of mechanisms are in place and operational. The opportunity to exercise choice should be provided to **Individuals** at the time of collection, and, on an ongoing basis, for subsequent uses or disclosure of **Personal Information**. The opportunity to exercise choice may be provided to the **Individual** after collection, but before: ● the **Participant,** its **Processors**, or any **Third Parties** make use of the **Personal Information**, when the purposes of such use are not related or compatible to the purposes for which the information was collected; and ● **Personal Information** is disclosed or distributed to **Third Parties**, other than **Processors**. Gaps and Remediation: If a mechanism is not provided, TRUSTe must inform the **Participant** that a mechanism for **Individuals** to exercise choice in relation to the use of their **Personal Information** must be provided.
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether	**11. Choice for Use or Disclosure of Sensitive Personal Information** Requirement: Obtain **Consent** (opt-in) from **Individuals** prior to using **Sensitive Personal Information** for unrelated purposes or disclosing it to **Third Parties**.

personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control** *2.9:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission (consent) where necessary and appropriate, and enable individual to opt out of ongoing processing. Data Privacy Framework Principles: II.2.c TRUSTe Data Privacy Framework Assessment Criteria 21 GDPR Articles 4(11), 6(1), and 9(2)	An organization is not required to obtain **Consent** (opt-in) with respect to **Sensitive Information** where the **Processing** is: ● in the vital interests of the **Individual** or another person; ● necessary for the establishment of legal claims or defenses; ● required to provide medical care or diagnosis; ● carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on the condition that the **Processing** relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a **Third Party** without the consent of the **Individual(s**); ● necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ● necessary to carry out the organization's obligations in the field of employment law; or ● related to data that are manifestly made public by the **Individual**. Evaluation: TRUSTe must verify that the **Participan**t provides a description of the mechanisms provided to **Individuals** so that they may exercise choice in relation to the use or disclosure of their **Sensitive Personal Information**, such as: ● online at point of collection; ● in person at the time of collection; ● via e-mail; ● via preference/profile page; ● via telephone; or ● via postal mail. TRUSTe must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used or disclosed. The opportunity to provide consent should be provided to the **Individual** at the time of collection. The opportunity to exercise choice may be provided to the **Individual** after collection, but before using **Sensitive Personal Information** for unrelated purpose or disclosing it to **Third Parties** not acting as **Processors** (e.g., agents, business associates, service providers, vendors). Gaps and Remediation: If TRUSTe finds that the **Participant's** mechanism to obtain consent is not displayed in a clear and conspicuous manner, TRUSTe must inform the **Participant** that all

	mechanisms that allow **Individuals** to provide consent in relation to the disclosure of their **Sensitive Personal Information**, must be clear and conspicuous in order to comply with this requirement. If **Consent (opt-in)** is not obtained, TRUSTe must inform the **Participant** that a mechanism to obtain **Consent** must be provided and that all mechanisms that allow **Individuals** to provide consent in relation to unrelated uses of or the disclosure of their **Sensitive Personal Information**, must be clear and conspicuous in order to comply with this requirement.
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control:** *2.9.1* Ensure consent is clear and conspicuous, freely given, and able to be withdrawn at any time. Data Privacy Framework Principles: II.2.a APEC CBPR Requirement: 17	**12. Clear and Conspicuous Access to Choice Mechanisms** Requirement: Display and provide choice mechanisms, which offer the **Individual** the ability to limit the, use or disclosure of their **Personal Information,** in a clear and conspicuous manner. Evaluation: TRUSTe must verify that the **Participant's** choice mechanism is displayed in a clear and conspicuous manner including that the choice mechanism is clear, written in plain language, conspicuous and presented in a manner that is distinguishable from other information presented to **Individuals**. Gaps and Remediation: If a choice mechanism is not provided, or when TRUSTe finds that the **Participant 's** choice mechanism is not displayed in a clear and conspicuous manner, TRUSTe must inform the **Participant** that all mechanisms that allow **Individuals** to exercise choice in relation to the use or disclosure of their **Personal Information** must be clear and conspicuous in order to comply with this requirement. Choice mechanisms must be clear, written in plain language, conspicuous and presented in a manner that is distinguishable from other information presented to **Individuals**.

TRUSTe Data Privacy Framework Assessment Criteria 20 GDPR Articles 7(2) and 7(4)	
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control:** *2.9.2* Ensure that evidence consent can be produced at any time. GDPR Article 7(1)	**13. Evidence of Consent** Requirement: The **Participant** must put in place controls and processes to ensure that evidence of the **Individual's** consent can be produced at any time. Evaluation: TRUSTe must verify the **Participant** has controls and processes in place to meet this requirement. Gaps and Remediation: If the **Participant** is not able to ensure that evidence of the **Individual's** consent can be produced at any time, TRUSTe must inform the **Participant** that the appropriate controls and processes must be put in place to meet this requirement.
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where	**14. Parental Consent** Requirement: If the **Participant** collects **Personal Information** directly from a child (as defined by applicable law), the **Participant** must obtain verifiable parental consent prior to collecting **Personal Information** directly from a child. Evaluation: TRUSTe must verify the **Participant** obtained verifiable parental consent prior to collecting **Personal Information** directly from a child.

necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control:** *2.10* If the individual is a child (as defined by applicable law), obtain verifiable parental consent for the processing. GDPR Article 8	Gaps and Remediation: If the **Participant** does not obtain verifiable parental consent prior to the collection of **Personal Information** directly from a child, TRUSTe must inform the **Participant** it must obtain verifiable parental consent.
TrustArc P&DG Standard: *Choice and Consent:* Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. **TrustArc P&DG Control:** *2.11* Provide mechanisms for individuals to easily opt-out of ongoing processing about them. GDPR Article 7(3)	**15. Right to Withdraw Consent** Requirement: The **Participant** must provide a mechanism by which the **Individual** may withdraw consent or change their choice selection, and to easily opt-out of ongoing process about them. Evaluation: TRUSTe must verify that the **Participan**t provides a mechanism to **Individuals** so that they may withdraw consent or change their choice selection, and to easily opt-out such as: ● online at point of collection; ● in person at the time of collection; ● via e-mail; ● via preference/profile page; ● via telephone; or ● via postal mail. TRUSTe must verify such a mechanism is in place and operational. Gaps and Remediation: If the **Participant** does not have an operational mechanism in place by which the **Individua**l may withdraw consent or change their choice selection, and to easily opt-out of ongoing process about them, TRUSTe must inform the **Participant** that an operational mechanism must be put in place to comply with this requirement.

ACCESS AND INDIVIDUAL RIGHTS Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Access and Individual Rights:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. **TrustArc P&DG Control** *2.12:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. Data Privacy Framework Principles: III.8.a.i.1 and III.8.f.i	**16. Right to Access** Requirement: The **Participant** must have available, operational, and understandable policies to enable **Individuals** to: • access and correct their **Personal Information** using mechanisms that are presented in a clear and conspicuous manner; and • obtain a copy of the corrected **Personal Information** or be provided confirmation that the data has been corrected or deleted. The **Participant** must grant access to any **Individual**, to **Personal Information** collected or gathered about that **Individual**, providing such request to **Personal Information** is reasonable and not excessive, upon receipt of sufficient information confirming the **Individual's** identity. The **Participant** should provide, at no cost to the **Individual**, a copy of the **Personal Information** that is processed in connection with the activity. The **Participant's** processes and mechanisms for access by **Individuals** must be simple and easy to use, presented in a clear and conspicuous manner, and be reasonable in regard to the manner of request and the nature of the **Personal Information**. The request must be responded to within a reasonable timeframe following an **Individual's** request for access (e.g., 45 days) and the **Personal Information** must be provided to **Individuals** in an easily comprehensible way. Access may be denied or limited under the following circumstances:

APEC CBPR Requirement: 36 TRUSTe Data Privacy Framework Assessment Criteria 36 GDPR Article 15	● where providing access would violate the legitimate rights of persons other than the **Individual**; ● where the burden or expense of providing access would be disproportionate to the risks to the **Individual**'s privacy; ● where providing access would reveal the **Participant's** own confidential commercial information—such as marketing inferences, classifications generated by the organization, or confidential commercial information of another that is subject to a contractual obligation of confidentiality; ● where providing access would interfere with the safeguarding of important countervailing public interests—such as national security, defense, or public security; ● where **Personal Information** is being **Processed** solely for research or statistical purposes; ● where providing access would interfere with the execution or enforcement of the law or with private causes of action—including the prevention, investigation, or detection of offenses or right to a fair trial; ● where providing access would breach a legal or other professional privilege or obligation; ● where providing access would prejudice employee security investigations or grievance proceedings or in connection with employee succession planning and corporate reorganizations; or ● where providing access would prejudice the confidentiality necessary in monitoring, inspection, or regulatory functions connected with sound management, or in future or ongoing negotiations involving the **Participant**. The **Participant** is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the **Individual** making the request. In addition, access needs to be provided only to the extent that the **Participant** stores the **Personal Information**. The **Participant** may set reasonable limits on the number of times within a given period that access requests from a particular **Individual** will be met. In setting such limitations, the **Participant** should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information. <u>Evaluation:</u> TRUSTe must verify that such policies are available, operational, and understandable.

	Gaps and Remediation: If the **Participant** does not have available, operational, and understandable policies in place and does not identify an applicable qualification, TRUSTe must inform the **Participant** that the existence of written procedures to respond to such requests is required for compliance with this requirement. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.
TrustArc P&DG Standard: *Access and Individual Rights:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. **TrustArc P&DG Control** *2.13 Enable individuals to rectify inaccurate personal data processed by the technology, process, or activity.* Data Privacy Framework Principles: III.8.a.i.2 TRUSTe Data Privacy Framework Assessment Criteria 37 GDPR Articles 16 and 19	**17. Right to Rectification** Requirement: Upon request, the **Participant** must enable **Individuals** to challenge the accuracy of the **Personal Information** that has been collected or held about the requesting **Individual** and have it rectified, completed, and/or amended. The **Participant** must rectify any inaccurate **Personal Information** collected or held by the requesting **Individual**, upon receipt of sufficient information confirming the **Individual's** identity. The **Participant** should communicate rectification of **Personal Information** to any recipients of the **Personal Information** to whom **Personal Information** have been disclosed, including any third party **Processors**. The **Participant's** processes or mechanisms for rectification of inaccurate **Personal Information** by the **Individual** must be simple and easy to use, presented in a clear and conspicuous manner, and reasonable in regard to the manner of request and the nature of the **Personal Information**. The request must be responded to within a reasonable timeframe following an **Individual's** request for correction (e.g., 45 days), and the **Personal Information** must be rectified and the **Individual** provided a copy of the corrected information. If the **Participant** denies correction to the **Individual's Personal Information**, it must explain to the **Individual** why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. Evaluation: TRUSTe must verify that the **Participant** has procedures in place to respond to such requests. TRUSTe must verify that such policies are available, operational, and understandable.

	Gaps and Remediation: If the **Participant** does not have a procedure for this, TRUSTe must inform the **Participant** that the existence of written procedures to respond to such requests is required for compliance with this requirement.
TrustArc P&DG Standard: *Access and Individual Rights:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. **TrustArc P&DG Control** *2.14 Where appropriate and in accordance with applicable law, enable individuals to delete personal data processed by the technology, process, or activity.* GDPR Articles 17 and 19	**18. Right to Erasure** Requirement: Where appropriate and in accordance with applicable law, the **Participant** must enable **Individuals** to delete **Personal Information** that is **Processed** by the **Participant** or **Third Parties** acting on the **Participant's** behalf (e.g., **Processors**). The **Participant** must delete **Personal Information** collected or held by the requesting **Individual**, upon receipt of sufficient information confirming the **Individual's** identity. The **Participant** should communicate obligations to delete **Personal Information** to any recipients of the **Personal Information** to whom **Personal Information** have been disclosed, including any third party **Processors**. The **Participant's** processes or mechanisms for deletion of **Personal Information** by the **Individual** must be simple and easy to use, presented in a clear and conspicuous manner, and, reasonable in regard to the manner of request and the nature of the **Personal Information**. The request must be responded to within a reasonable timeframe following an **Individual's** request for deletion (e.g., 45 days), and the **Personal Information** must be deleted and the **Individual** provided confirmation of such deletion. TRUSTe must verify that such policies are available, operational, and understandable. The **Participant** is not required to delete the **Individual's Personal Information** if **Processing** is necessary for: ● exercising the right of freedom of expression and information; ● compliance with a legal obligation which requires processing by applicable law to which the **Participant** or **Controller** is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the **Controller**; ● reasons of public interest in the area of public health; ● archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where it is likely to render impossible or seriously impair the achievement of the objectives of that processing; or ● the establishment, exercise, or defense of legal claims.

	Evaluation: TRUSTe must verify the **Participant** has procedures in place to respond to such requests. If the **Participant** identifies an applicable qualification to not delete **Individuals' Personal Information**, TRUSTe must verify whether the applicable qualification is justified. Gaps and Remediation: If the **Participant** does not have a procedure for this and the **Participant** does not identify an acceptable qualification, TRUSTe must inform the **Participant** that the existence of written procedures to respond to such requests is required for compliance with this requirement.
TrustArc P&DG Standard: *Access and Individual Rights:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. **TrustArc P&DG Control** *2.15 Enable individuals to request reasonable restrictions on uses or disclosures of personal data about them where such restrictions do not adversely affect the rights of others, do not require disproportionate efforts for the organization to implement, or where required by law.*	**19. Right to Restrict Processing** Requirement: Upon request, the **Participant** must enable **Individuals** to restrict the **Processing** or disclosure of their **Personal Information** where appropriate and in accordance with applicable law. Such restrictions must not adversely affect the rights of other **Individuals** or require disproportionate efforts for the **Participant** to implement. The **Participant** must restrict the **Processing** or disclosure of **Personal Information** collected or held by the requesting **Individual**, upon receipt of sufficient information confirming the **Individual's** identity. If **Personal Information** has been disclosed to any third parties, the **Participant** should communicate the restriction. The **Participant's** processes or mechanisms to receive requests to restrict the **Processing** or disclosure of **Personal Information** by the **Individual** must be reasonable in regard to the manner of request and the nature of the **Personal Information**. The request must be responded to within a reasonable timeframe (e.g., 45 days) and the **Individual** provided confirmation that their request has been filled. The **Participant** may deny the **Individual's** request if the requested restriction will: ● adversely affect the rights of other **Individuals;** or ● require disproportionate efforts for the **Participant** to implement.

GDPR Articles 18 and 19	Evaluation: TRUSTe must verify the **Participant** has procedures in place to respond to such requests. If the **Participant** identifies an applicable qualification to restrict processing or disclosure of **Individuals' Personal Information**, TRUSTe must verify whether the applicable qualification is justified. Gaps and Remediation: If a mechanism is not provided and the **Participant** does not identify an acceptable qualification, TRUSTe must inform the **Participant** that a mechanism for **Individuals** to request the restriction to the **Processing** or disclosure of their **Personal Information** must be provided.
TrustArc P&DG Standard: *Access and Individual Rights:* Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated. **TrustArc P&DG Control** *2.16 Where reasonable and practicable, enable individuals to access information about themselves in a machine-readable or electronic format consistent with its intended use.* GDPR Article 20	**20. Right to Data Portability** Requirement: Where reasonable and practicable, the **Participant** must provide a mechanism to enable **Individuals** to access information about themselves in a machine-readable or electronic format consistent with its intended use unless it will adversely affect the rights of other **Individuals** or the information is not processed by an automated means. Evaluation: TRUSTe must verify such a mechanism is in place. Gaps and Remediation: If the **Participant** does not have such a mechanism in place by which the **Individua**l may access information about themselves in a machine-readable or electronic format, TRUSTe must inform the **Participant** that such a mechanism must be put in place to comply with this requirement.

DATA INTEGRITY AND QUALITY Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Data Integrity and Quality:* Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use. **TrustArc P&DG Control** *2.17:* Assure that data are kept sufficiently accurate, complete, relevant, and current consistent with its intended use. Data Privacy Framework Principles: II.5.a APEC CBPR Requirement: 21 TRUSTe Data Privacy Framework Assessment Criteria 34	**21. Data Integrity and Quality** Requirement: The **Participant** must take steps to verify that the **Personal Information** held is up to date, accurate, and complete, to the extent necessary for the purpose(s) of use. TRUSTe must require the **Participant** to provide the procedures the **Participant** has in place to verify and ensure that the **Personal Information** held is up to date, accurate, and complete, to the extent necessary for the purposes of use. Evaluation: TRUSTe will verify that reasonable procedures are in place to allow the **Participant** to maintain **Personal Information** that is up to date, accurate, and complete, to the extent necessary for the purpose of use. Gaps and Remediation: If the **Participant** does not have a reasonable procedure in place, TRUSTe must inform the **Participant** that procedures to verify and ensure that the **Personal Information** held is up to date, accurate, and complete, to the extent necessary for the purposes of use, are required for compliance with this requirement.

GDPR Article 5(1)(d)	

SECURITY Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. **TrustArc P&DG Control** *2.18:* Put in place administrative, physical, and technical safeguards to protect data from loss, misuse and unauthorized access, disclosure, alteration, or destruction. Data Privacy Framework Principles: II.4.a	22. **Security of Processing** Requirement: the **Participant** must implement reasonable physical, technical, and administrative safeguards to protect **Personal Information** against risks such as loss or unauthorized access, destruction, use, modification, disclosure of information, or other misuses. The **Participant** must implement reasonable administrative, technical, and physical safeguards, suitable to the **Participant's** size and complexity, the nature and scope of its activities, and the sensitivity of the **Personal Information** it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened, the sensitivity of the information, and the context in which it is held. The **Participant** must take reasonable measures to require information **Processors** (e.g., agents, business associates, service providers, vendors) to which **Personal Information** is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure, or other misuses of the information. These safeguards may include:

APEC CBPR Requirement: 27 TRUSTe Data Privacy Framework Assessment Criteria 28 GDPR Article 32(1), GDPR Article 32(2) ISO 27001 8.1 Operational Planning and Control and 8.3 Information Security Risk Treatment	● authentication and access control (e.g., password protections, access management, limiting network and system access to authorized **Individuals**); ● **Pseudonymisation** and encryption; ● removable media controls including management, disposal and transfer; ● boundary protection (e.g., firewalls, intrusion detection); ● physical and environmental security controls; ● data backup and disaster recovery procedures; ● secure data disposal procedures; ● audit logging; or ● monitoring (e.g., external and internal audits, vulnerability scans). The **Participant** must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Evaluation: TRUSTe must verify the existence of such safeguards and that those safeguards are adequate and proportional to the probability and severity of the harm threatened, the sensitivity of the information, and the context in which it is held. Gaps and Remediation: If the **Participant** has no physical, technical, and administrative safeguards, or inadequate safeguards to protect **Personal Information**,TRUSTe must inform the **Participant** that the implementation of such safeguards are required for compliance with this requirement.
TrustArc P&DG Standard: *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. **TrustArc P&DG Control** *2.18:* Put in place administrative, physical, and technical safeguards to protect data from loss,	23. ***Incident Detection.*** Requirement: the **Participant** must have incident detection, escalation, and management procedures in place, and mechanisms to determine whether an incident involves **Personal Information**. Evaluation: TRUSTe must verify that the **Participant** has incident detection, escalation, and management procedures in place, and mechanisms to determine whether an incident involves **Personal Information**.

misuse and unauthorized access, disclosure, alteration, or destruction. GDPR Articles 33-34 ISO 27001 8.1 Operational Planning and Control	Gaps and Remediation: If the **Participant** does not have these procedures and mechanisms in place, TRUSTe must inform the **Participant** that these procedures and mechanisms must be in place to meet this requirement.
TrustArc P&DG Standard: *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. **TrustArc P&DG Control** *2.19* Conduct security risk assessments as required by the security program, and remediate areas of identified risk. GDPR Article 32(2) ISO 27001 8.2 Information Security Risk assessment and 8.3 Information Security Risk Treatment	24. **Security Risk Assessments** Requirement: The **Participant** must conduct security risk assessments as required by its security program, and remediate areas of identified risk. Evaluation: TRUSTe must verify the **Participant** has policies and procedures in place for conducting these assessments, and remediating areas of identified risk. Gaps and Remediation: If the **Participant** does not have policies and procedures in place for conducting these assessments, and remediating areas of identified risks, then TRUSTe must inform the **Participant** that such policies and procedures must be put in place to comply with this requirement.

TRANSPARENCY Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Transparency*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. **TrustArc P&DG Control** *2.20*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights, including those arising out of data-related incidents and breaches. Data Privacy Framework Principles: II.1.a.ii APEC CBPR Requirement: 1a	**25. Comprehensive Privacy Notice** Requirement: The **Participant** must provide the **Individual** a **Privacy Notice** in clear and plain language that informs **Individuals** of the following: ● a definition of the scope of the **Privacy Notice;** ● the identity of the **Participant** (e.g., company name), and, where applicable, the identity of affiliates, subsidiaries, or joint **Controllers** collecting **Personal Information**; ● the types of entity(ies) other than the **Participant**, including **Processors**, collecting **Personal Information**; ● the types of **Personal Information** collected, whether collected directly through active or passive means or through a third party or agent; ● the processing purposes for which **Personal Information** was collected; ● whether their **Personal Information** is disclosed to **Third Parties** and for what purpose(s); **Third Parties** include **Controllers** (e.g., advertising networks, marketing partners) and **Processors** (e.g., agents, business associates, service providers, vendors) acting on the **Participant's** behalf; ● whether and how an **Individual** can exercise their Individual rights including: ○ requesting access and correct their **Personal Information;** ○ rectifying, completing, and/or amending inaccurate or incomplete information about themselves; ○ requesting deletion of their **Personal Information;** ○ restricting the processing or disclosure of their **Personal Information;** or ○ requesting **Personal Information** in a machine readable format; ● the choices and means available for limiting the use and disclosure of **Personal Information,** including how **Individuals** can change their preferences;

TRUSTe Data Privacy Framework Assessment Criteria 3, 4, 6-11, & 15 GDPR Article 13(1) and 13(2), GDPR Article 14(1) and 14(2)	● a general description of the **Participant's** information retention policies, and the types of information security measures in place to protect **Personal Information**; ● that collected information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the **Participant** merges with or is acquired by a **Third Party**, or goes bankrupt; ● a description of the method for notification of any **Material Change**s in the **Participant's** privacy practices; ● how to contact the **Participant's** organization with any inquiries or complaints about its privacy practices or compliance with its **Privacy Notice;** ● the independent dispute resolution body designated to address complaints; and ● the effective date of the **Privacy Notice**. Evaluation: TRUSTe must verify the **Participant** is providing **Individuals** the required information in its **Privacy Notice**. Gaps and Remediation: If this information is not provided and the **Participant** does not identify an applicable qualification, TRUSTe must inform the **Participant** that notice that **Personal Information** is being collected is required for compliance with this requirement. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified. See Assessment Criteria 26 for a list of applicable qualifications.
TrustArc P&DG Standard: *Transparency:* Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. **TrustArc P&DG Control**	**26. Provision of Privacy Notices** Requirement: Provide clear and conspicuous notice(s) about the practices and policies that govern the **Personal information** described above in Assessment Criteria 25 (e.g., a **Privacy Notice**) and effective date of such notice. The **Participant** must provide copies of all applicable **Privacy Notices** and/or hyperlinks to the same. **Participant** must always provide such notice: ● before it uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization; or

2.20.1: Ensure information about data processing and individuals rights is clear and conspicuous. Data Privacy Framework Principles: II.1.b APEC CBPR Requirement: 1 TRUSTe Data Privacy Framework Assessment Criteria 17 GDPR Articles 12 - 14	● discloses it for the first time to a **Third Party** not acting as a **Processor**. Where applicable, at least one notice is made available on the **Participant's** website, such as text on a web page, link from URL, attached document, pop-up window, included on frequently asked questions (FAQs), or other (must be specified): ● is easy to find and accessible; ● applies to **Personal Information** in the defined scope of the notice, whether collected online or offline. Notice is not required when: ● **Personal information** is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives; ● **Personal Information** is obtained by investment bankers and auditors for the purpose of conducting due diligence as part of a merger or acquisition; or ● **Personal Information** is available through public sources of information and has been not combined with information from non-public sources or is subject to restrictions; or. ● **Personal Information** must remain confidential subject to an obligation of professional secrecy regulated by applicable law, including a statutory obligation of secrecy. Evaluation: TRUSTe must verify that **Participant's** applicable **Privacy Notices** are made available when individuals are first asked to provide **Personal Information** to the **Participant** or as soon thereafter as is practicable. Gaps and Remediation: If the **Participant** is unable to provide this information, TRUSTe must inform the **Participant** that notice as described herein is required for compliance with this principle. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.
TrustArc P&DG Standard: *Transparency:* Inform individuals about the ways in which data about them are processed and how to	**27. *Timing of Notice*** Requirement: At the time of collection of **Personal Information** (whether directly or through the use of **Third Parties** acting on the **Participant's** behalf) or as soon as thereafter is practicable, the **Participant** must provide notice that such information is being collected.

exercise their data-related rights. **TrustArc P&DG Control** *2.20.2:* Ensure information about data processing and individuals rights is provided before information is collected from individuals, at the time of collection, or as soon as practicable thereafter. Data Privacy Framework Principles: II.1.b APEC CBPR Requirement: 2 TRUSTe Data Privacy Framework Assessment Criteria 18 GDPR Articles 13 and 14	If notice is provided after the collection of **Personal Information,** it must be provided before the organization uses such information for a purpose other than that for which it was originally collected or **Processed** by the transferring organization or before the organization discloses it for the first time to a **Third Party.** Evaluation: TRUSTe must verify that the **Participant**; ● provides notice to **Individuals** that their **Personal Information** is being (or, if not practicable, has been) collected and that the notice is reasonably available to **Individuals**; and ● does not, in any event, use any **Personal Information** for a purpose other than that for which it was originally collected or processed by the transferring organization, or disclose it for the first time to a **Third Party** without first providing notice. Gaps and Remediation: If this information is not provided and the **Participant** does not identify an applicable qualification, TRUSTe must inform the **Participant** that notice that **Personal Information** is being collected is required for compliance with this principle. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified. See Assessment Criteria 26 for a list of applicable qualifications.

AWARENESS AND TRAINING Communicate expectations, and provide general and contextual training.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Awareness and Training:* Communicate expectations. Provide general and contextual training **TrustArc P&DG Control** *1.7*: Communicate about the value and risks associated with data as well as program and process expectations. Provide both general and contextual training, including professional certification training. Reinforce messages periodically. Data Privacy Framework Principles: II.4.a and III.7.c APEC CBPR Requirement: 29	28. **Awareness and Training** Requirement: The **Participant** must make its employees aware of the importance of maintaining the privacy and security of **Personal Information** (e.g., through regular training and oversight). Evaluation: TRUSTe must verify that the **Participant's** employees are aware of the importance of, and obligations respecting, maintaining the privacy and security of **Personal Information** through regular training and oversight as demonstrated by procedures, which may include: ● training program for employees; ● regular staff meetings or other communications; or ● security policy signed by employees. Gaps and Remediation: If the **Participant** does not make employees aware of the importance of, and obligations respecting, maintaining the privacy and security of **Personal Information** through regular training and oversight, TRUSTe has to inform the **Participant** that the existence of such procedures are required for compliance with this requirement.

TRUSTe Data Privacy Framework Assessment Criteria 30 GDPR Article 32(1)(d) ISO 27001 7.3 Awareness and 7.4 Communication	

MONITORING AND ASSURANCE Companies must continually monitor, and periodically assess and audit the effectiveness of controls and risk-mitigation initiatives.	
TrustArc P&DG Framework and External Regulatory Standard Mapping	**Assessment Criteria**
TrustArc P&DG Standard: *Monitoring and Assurance:* Companies must continually monitor, and periodically assess and audit the effectiveness of controls and risk-mitigation initiatives. **TrustArc P&DG Control** *3.1*: Continually monitor and periodically evaluate program maturity, and periodically assess and audit the effectiveness of program controls and risk-mitigation initiatives. GDPR Articles 35(2) and 39(1)(c)	29. ***Privacy Reviews.*** Requirement: The **Participant** must have mechanisms in place to assess and document processing activity risk and control effectiveness, and have processing activity risk and controls, such as PIAs and DPIAs, reviewed by a Chief Privacy Officer (CPO) or other privacy leader. Evaluation: TRUSTe will verify the **Participant** has mechanisms in place to assess and document, and have processing activity risk and controls reviewed by a CPO or other privacy leader. Gaps and Remediation: If the **Participant** does not have mechanisms in place, then TRUSTe must inform the **Participant** that a process to assess and document, and have processing activity risk and controls reviewed by a CPO or other privacy leader must be in place to meet this requirement.

III. DEFINITIONS

“Controller” is the entity that, alone or jointly with others, determines the purpose of collecting data, how it’s used, and who has access to it.

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

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

“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.

"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, or online identifier) or through other factors (e.g., genetic, physical, or social identity).

“Personal Information Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **Personal Information** transmitted, stored or otherwise processed.

“Processing” of **Personal Information** means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

"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.

“Processor” is an entity that processes data on behalf of another entity, or 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 know as agents, business associates, service providers acting as an agent or vendor, or vendors.

“Pseudonymization” is the processing of **Personal Information** in such a manner that the **Personal Information** can no longer be attributed to a specific **Individual** without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the **Personal Information** is not attributed to an identified or identifiable natural person.

“Sensitive Personal Information” is information that if accessed, used, or disclosed without authorization would be reasonably or foreseeably likely to cause financial, physical, discriminatory, or reputational harm to an **Individual**.

Examples of Sensitive Information include:

- racial or ethnic origin of the **Individual**;
- political opinions of the **Individual**;
- religious, philosophical, or similar beliefs or activities of the **Individual**;
- **individual’s** trade union membership or activities;
- precise information regarding the **Individual’s** past, present, or future physical or mental health condition and treatments including genetic, genomic, and family medical history;
- information regarding the **Individual’s** sexual life or orientation; or
- the commission or alleged commission of any offense by the **Individual**.

“Third Party” is an entity other than the **Participant** or the **Individual** that either is not a subsidiary or affiliate under common control with the **Participant**, or is not acting solely as a **Processor** for the **Participant**.