TRUSTe Data Privacy Framework Verification Program Assessment Criteria

I. INTRODUCTION **2**

II. ASSESSMENT CRITERIA **4**

NOTICE 4

CHOICE 16

ACCOUNTABILITY FOR ONWARD TRANSFER 21

SECURITY 26

DATA INTEGRITY AND PURPOSE LIMITATION 29

ACCESS 33

RECOURSE, ENFORCEMENT, AND LIABILITY 37

HUMAN RESOURCES DATA 39

PHARMACEUTICAL AND MEDICAL PRODUCTS 40

III. DEFINITIONS **44**

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 and the unique requirements of the regulatory standard upon which a certain program is based.

The TRUSTe Data Privacy Framework Verification Programs ("the Program”) is designed to enable organizations, in preparation for self-certification with the U.S. Department of Commerce (DOC) , to assess and obtain verification from TRUSTe, as an outside compliance reviewer, that their privacy and data governance practices for personal information comply with the principles set forth in the 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. The assessment criteria set forth in this document are aligned with the principles laid out in the 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 (collectively herein, the “Data Privacy Framework”).

The Assessment Criteria are organized by the core seven Data Privacy Framework Principles of:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement, and Liability

There are two additional sections included in these Assessment Criteria that address the requirements of Supplemental Principle 9, which applies to Human Resources Data, and Supplemental Principle 14, which applies to data used for Pharmaceutical and Medical Products and Research.

Each section contains the Assessment Criteria TRUSTe uses to assess an organization's compliance with the principle. Any differences between the 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 are noted within the Assessment Criteria.

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 verification processes, and self-certification with the DOC, organizations participating in this Program will be issued and authorized to display the TRUSTe Privacy Verification Program seal.

Defined terms appear in **bold.**

II. ASSESSMENT CRITERIA

NOTICE

The purpose of the Notice Principle is to ensure that **Individuals** understand an organization's **Personal Information** policies, including its participation in Data Privacy Framework, the purposes for which it collects **Personal Information**, and to whom it may disclose **Personal Information**. The Notice Principle is not absolute and is subject to exceptions. Refer to the Data Privacy Framework Assessment Criteria, below, for a list of exceptions.

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. Data Privacy Framework Principles: II.1.a.i	**1. Data Privacy Framework Participation Statement** Requirement: The **Privacy Notice** must explicitly inform **Individuals** of the organization's participation in the EU-U.S. Data Privacy Framework and, as applicable, UK Extension to the EU-U.S. Data Privacy Framework, and/or Swiss-U.S. Data Privacy Framework, and the scope of its participation. Evaluation: TRUSTe must verify that the **Participant** provides accurate notice to **Individuals** of its participation in and explicitly state its participation in the EU-U.S. Data Privacy Framework and, as applicable, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S, Data Privacy Framework. Gaps and Remediation: If the **Privacy Notice** does not provide this information, TRUSTe must notify the **Participant** that notice of its participation in Data Privacy Framework and specification of participation in EU-U.S. Data Privacy Framework and, as applicable, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework is required and must be included in its Privacy Notice at the time of application and for the duration of its self-certification to the Data Privacy Framework.

	If **Participants** do not complete the self-certification process with the DOC, **Participants** are responsible for promptly removing references in its **Privacy Notice** to Data Privacy Framework participation.
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. Data Privacy Framework Principles: II.1.a.i	**2. Link to Data Privacy Framework List** Requirement: The **Privacy Notice** must provide a link to or the web address for the Data Privacy Framework List. The link that must be included in order to meet this requirement is https://www.dataprivacyframework.gov/s/. Evaluation: TRUSTe must verify that the **Participant** provides a link to or the web address for the Data Privacy Framework List, and that it goes to https://www.dataprivacyframework.gov/s/. Gaps and Remediation: If the link is not provided, TRUSTe must notify the **Participant** that a link to the web address for the Data Privacy Framework List (https://www.dataprivacyframework.gov/s/) is required and must be included in the **Privacy Notice**.
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. Data Privacy Framework Principles: II.1.a.ii APEC CBPR Requirement: 1a Enterprise Practicest Assessment Criteria: 25	**3. Description of How Personal Information is Collected** Requirement: The **Privacy Notice** must describe how **Personal Information** is collected. Evaluation: TRUSTe must verify that: ● the **Privacy Notice** describes that the collection practices and policies apply to all covered **Personal Information** collected by the **Participant**; ● the **Privacy Notice** indicates what types of **Personal Information**, whether collected directly or through a third party or agent, are collected; and ● the **Privacy Notice** reports the categories or specific sources of all categories of **Personal Information** collected. Gaps and Remediation: If the **Privacy Notice** does not describe how **Personal Information** is collected, TRUSTe must inform the **Participant** that the **Privacy Notice** must provide the information as described herein for compliance with this Principle.

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. Data Privacy Framework Principles: II.1.a.ii CBPR Intake Questionnaire General *(ii)* Enterprise Practices Assessment Criteria: 25	**4. Information Regarding Other Entities or Subsidiaries** Requirement: The **Privacy Notice** must provide information regarding other entities or subsidiaries of **Participant's** organization that also adhere to Data Privacy Framework. Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** of any entities or subsidiaries of the organization also adhering to Data Privacy Framework. Gaps and Remediation: If the **Privacy Notice** does not include this information, TRUSTe must notify the **Participant** that the **Privacy Notice** should disclose any entities or subsidiaries of the organization that are also adhering to Data Privacy Framework.
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. Data Privacy Framework Principles: II.1.a.iii	**5. Commitment to the Data Privacy Framework Principles** Requirement: The **Privacy Notice** must inform **Individuals** about the organization's commitment to be subject to the Principles all **Personal Information** received in reliance on EU-U.S. Data Privacy Framework and, as applicable, UK Extension to the EU-U.S. Data Privacy Framework and/or Swiss-U.S. Data Privacy Framework. ● For **Personal Information** received from the EU, **Participant** must commit to subject that information to the EU-U.S. Data Privacy Framework Principles. ● For Personal Information received from the UK, Participant must commit to subject that information to the EU-U.S. Data Privacy Framework Principles pursuant to the UK Extension to the EU-U.S. Data Privacy Framework. ● For **Personal Information** received from Switzerland, **Participant** must commit to subject that information to the Swiss-U.S. Data Privacy Framework Principles..

	Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** of its commitment to subject to the Principles all **Personal Information** received from either the EU, and as applicable, the UK and/or Switzerland in reliance on the respective Data Privacy Framework. If the **Participant** is relying on the UK Extension to the EU-U.S. Data Privacy Framework for information received from the UK, the **Participant** must also be a **Participant** in the EU-U.S. Data Privacy Framework. Gaps and Remediation: If the Privacy Notice does not disclose this,TRUSTe must notify the Participant that notice of its commitment to subject to the Principles all Personal Information received from the EU, and as applicable, the UK and/or Switzerland in reliance on the Data Privacy Framework Principle is required and must be included in the **Privacy Notice.**
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. Data Privacy Framework Principles: II.1.a.iv APEC CBPR Requirement: 1b Enterprise Practices Assessment Criteria: 25	**6. Description of Personal Information Collection Purposes** Requirement: The **Privacy Notice** must describe the purpose(s) for which **Personal Information** is collected. Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** of the purpose(s) for which **Personal Information** is being collected. Gaps and Remediation: If the **Privacy Notice** does not describe this, TRUSTe must notify the **Participant** that notice of the purpose(s) for which **Personal Information** is collected is required and must be included in their **Privacy Notice**.
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.	**7. Information Regarding the Use and Disclosure of Personal Information** Requirement: The **Privacy Notice** must provide information regarding the use and disclosure of an **Individual's Personal Information.**

Data Privacy Framework Principles: II.1.a.iv APEC CBPR Requirement: 1e Enterprise Practices Assessment Criteria: 25	Evaluation: TRUSTe must verify that the **Participant's Privacy Notice** includes, if applicable, information regarding the use and disclosure of all **Personal Information** collected. Gaps and Remediation: If the **Privacy Notice** does not provide information regarding the use and disclosure of the **Individual's Personal Information**, TRUSTe must inform the **Participant** that such information is required for compliance with this principle.
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. Data Privacy Framework Principles: II.1.a.v Enterprise Practices Assessment Criteria: 25	**8. Contact Information** Requirement: The **Privacy Notice** must inform **Individuals** about how to contact the **Participant's** organization with any inquiries or complaints about its privacy practices or compliance with the Data Privacy Framework Principles. If the **Participant** has an establishment in the EU, the UK and/or Switzerland that can respond to such complaints or inquiries from **Individuals** located in one of those respective areas, contact information for that establishment must be included in the **Privacy Notice.** Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** about how to contact the organization with any inquiries or complaints regarding its privacy practices or compliance with the Principles, including any relevant establishment in the EU, the UK, and/or, Switzerland that can respond to such inquiries or complaints. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that notice about how to contact the organization with any inquiries or complaints regarding the organization's privacy practices or compliance with the Principles, including any relevant establishment in the EU, the UK and/or Switzerland that can respond to such inquiries or complaints, is required and must be included in their **Privacy Notice**.
TrustArc P&DG Standard: *Transparency*: Inform individuals about the ways in which data about them are processed and	**9. Description of Personal Information Disclosure to Third Parties** Requirement: The **Privacy Notice** must inform **Individuals** about whether their **Personal Information** is disclosed to **Third Parties** and for what purpose(s).

how to exercise their data-related rights. Data Privacy Framework Principles: II.1.a.vi APEC CBPR Requirement: 1c Enterprise Implement Assessment Criteria: 25	**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. Evaluation: TRUSTe must verify that the **Participant** includes information about whether **Individuals' Personal Information** will or may be made available to **Third Parties**, identifies the categories or specific **Third Parties**, and the purpose(s) for which the **Personal Information** will or may be made available. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that the notice must describe whether **Individuals' Personal Information** will or may be made available to **Third Parties**, identifies the categories or specific **Third Parties**, and the purpose(s) for which the **Personal Information** will or may be made available.
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. Data Privacy Framework Principles: II.1.a.vii APEC CBPR Requirement: 1f Enterprise Practices Assessment Criteria: 25	**10. Information Regarding Access and Correction** Requirement: The **Privacy Notice** must provide information regarding whether and how an **Individual** can access and correct their **Personal Information.** See Assessment Criteria 36 for a list of applicable qualifications to the Access Principle and when this information does not have to be provided. Evaluation: TRUSTe must verify that the **Privacy Notice** includes: ● the process through which an **Individua**l may access his or her **Personal Information** (including electronic or traditional non-electronic means); and ● the process that an **Individual** must follow in order to correct his or her **Personal Information**. Gaps and Remediation: If the **Privacy Notice** does not contain this information and the **Participant** does not identify an applicable qualification, TRUSTe must inform the **Participant** that providing information about access and correction, including the **Participant's** typical

	response time for access and correction requests, 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 exercise their data-related rights. Data Privacy Framework Principles: II.1.a.viii Enterprise Practices Assessment Criteria: 25	**11. Information Regarding Choice** Requirement: The **Participant's Privacy Notice** must inform **Individuals** of the choices and means available for limiting the use and disclosure of **Personal Information.** See Assessment Criteria 19 & 21 for a list of applicable qualifications to the Choice Principle and when this information does not have to be provided. Evaluation: TRUSTe must verify that the **Participant's Privacy Notice** includes information about the choices and means available to **Individuals** for limiting the use and disclosure of their **Personal Information**. Gaps and Remediation: If the **Privacy Notice** does not contain this information and the **Participant** does not identify an applicable qualification, TRUSTe must notify the **Participant** that notice about the choices and means the organization offers **Individuals** for limiting the use and disclosure of their **Personal Information** is required and must be included in their **Privacy Notice**. 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 exercise their data-related rights. Data Privacy Framework Principles: II.1.a.ix	**12. Independent Dispute Resolution Information** Requirement: The **Privacy Notice** must inform **Individuals** of the independent dispute resolution body designated to address complaints free of charge to Individuals and whether it is: (1) the panel established by EU data protection authorities (EU DPAs), the UK Information Commissioner's Office (ICO), or the Swiss Federal Data Protection and Information Commissioner (FDPIC), (2) an alternative dispute resolution provider based in the EU, the UK, and/or Switzerland or (3) an alternative dispute resolution provider based in the United States. For Participants in this program, TRUSTe requires TRUSTe to be listed as the Participant's U.S.-based independent dispute resolution body designated to address complaints relating to Personal Information excluding human resources data.

	For human resources data, the panel established by the data protection authorities (EU DPAs) for EU-based employees, the Information Commissioner's Office (ICO) for employees located in the UK, or the Swiss Federal Data Protection and Information Commissioner (FDPIC) for employees located in Switzerland must be listed as the independent dispute resolution mechanism in the **Privacy Notice**. For any other types of **Personal Information** that make use of TRUSTe's Dispute Resolution & Privacy Feedback Mechanism in fulfillment of Data Privacy Framework's Independent Dispute Resolution Mechanism requirement, **Participant** must provide a link to TRUSTe's Dispute Resolution & Privacy Feedback mechanism, and a statement that the provider is based in the U.S. and recourse is free of charge to **Individuals** in its **Privacy Notice.** Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** about the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the **Individual**. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that: ● notice of the independent dispute resolution body designated to address complaints; ● notice that the recourse is free of charge to **Individuals**; and ● notice of the type of independent dispute resolution provider and whether the provider is U.S.-based are required and must be included in their **Privacy Notice**.
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. Data Privacy Framework Principles: II.1.a.x	**13. U.S. Statutory Oversight Information** Requirement: The **Privacy Notice** must inform **Individuals** about which U.S. statutory oversight the **Participant** is subject to. Organizations under the oversight of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT) may participate in the Data Privacy Framework. Other U.S. statory bodies with regulatory oversight have not been recognized by the EU, the UK, and/or Switzerland at this time.

	Evaluation: TRUSTe must verify that the **Participant** provides notice to **Individuals** about being subject to the investigatory and enforcement authority of the FTC or the DoT. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that the notice must inform **Individuals** about which U.S. statutory oversight body the organization is subject to.
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. Data Privacy Framework Principles: II.1.a.xi	**14. Binding Arbitration** Requirement: The **Privacy Notice** must inform **Individuals** about the possibility for them, under certain conditions, to invoke binding arbitration. Evaluation: TRUSTe must verify that the **Participant's Privacy Notice** includes information informing **Individuals** about the possibility that under certain circumstances they may invoke binding arbitration. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that notice about the possibility, under certain circumstances, for the **Individual** to invoke binding arbitration is required and must be included in their **Privacy Notice**.
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. Data Privacy Framework Principles: II.1.a.xii APEC CBPR Requirements: 4 and 45	**15. Disclosing Personal Information in Response to Lawful Requests** Requirement: The **Privacy Notice** must inform **Individuals** of the **Participant** organization's obligation to disclose **Personal Information** in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Evaluation: TRUSTe must verify that the **Participant's Privacy Notice** informs **Individuals** about its obligation to disclose **Personal Information** in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that notice about its requirement to disclose **Personal Information** in

Enterprise Practices Assessment Criteria: 25	response to lawful requests by public authorities, including to meet national security or law enforcement requirements, is required and must be included in their **Privacy Notice**.
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. Data Privacy Framework Principles: II.1.a.xiii	**16. Onward Transfer Liability** Requirement: The **Privacy Notice** must inform **Individuals** of the organization's liability in cases of onward transfers to **Third Parties.** Evaluation: TRUSTe must verify that the **Participant** provides information regarding its liability in cases of onward transfers to **Third Parties** (e.g., **Participant** is responsible for the **Processing** of **Personal Information** by its **Third-Party Processors**). Gaps and Remediation: If the **Privacy Notice** does not contain this information, TRUSTe must notify the **Participant** that the **Privacy Notice** must include information regarding the **Participant's** liability in the case of onward transfer to **Third Parties**.
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. Data Privacy Framework Principles: II.1.b APEC CBPR Requirement: 1 Enterprise Practices Assessment Criteria 25 & 26	**17. 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 3 (e.g., a **Privacy Notice**) and effective date of such notice. **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 ● 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 in accordance with the principles of the Data Privacy Framework; ● is easy to find and accessible;

	● applies to **Personal Information** in the defined scope of the notice, whether collected online or offline. The **Participant** must provide copies of all applicable **Privacy Notices** and/or hyperlinks to the same. Under Data Privacy Framework, 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. Evaluation: TRUSTe must verify that **Participant's** applicable **Privacy Notices** are made available when individuals are first asked to provide personal information to the organization 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 exercise their data-related rights. Data Privacy Framework Principles: II.1.b	**18. 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. 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

APEC CBPR Requirement: 2 Enterprise Practices Assessment Criteria 27	collected or processed by the transferring organization or before the organization discloses it for the first time to a **Third Party.** 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 nonpublic sources or is subject to restrictions. 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 providing notice of **Personal Information** collection at the time of collection or as soon as thereafter is required for compliance with this principle. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.

CHOICE

The purpose of the Choice Principle is to ensure that **Personal Information** is used and disclosed in ways that are consistent with an **Individual's** expectations. Organizations must give **Individuals** the choice to "opt-out" of having their **Personal Information** used or disclosed to **Third Parties** acting as **Controllers**. When using or disclosing **Sensitive Personal Information**, organizations must obtain "opt-in" **Express Consent**. The Choice Principle is not absolute and is subject to exceptions. Refer to the Data Privacy Framework Assessment Criteria, below, for a list of exceptions.

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. Data Privacy Framework Principles: II.2.a.i APEC CBPR Requirement: 15 & 16 Enterprise Practices Assessment Criteria 10	**19. 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.** 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. 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**. 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 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; ● **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** is disclosed in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Evaluation: 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, for subsequent uses or disclosure of **Personal Information**. If the **Participant** identifies an applicable qualification to the provision of choice, 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 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 personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. Data Privacy Framework Principles: II.2.a APEC CBPR Requirement: 17 Enterprise Practices Assessment Criteria 12	**20. Clear and Conspicuous Access to Choice Mechanisms** Requirement: Display and provide choice mechanisms, which offer the Individual the ability to limit the collection, use, and/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 collection, use, and/or disclosure of their **Personal Information** must be clear and conspicuous in order to comply with this principle. Choice mechanisms must be clear, written in plain language, conspicuous and presented in a manner that is distinguishable from other information presented to **Individuals**.
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.	**21. Choice for Use or Disclosure of Sensitive Personal Information** Requirement: Obtain affirmative **Express Consent** (opt-in) from **Individuals** prior to use or disclosure of **Sensitive Personal Information** to **Third Parties**. Subject to the qualifications outlined below, the opportunity to for **Individuals** to provide **Express Consen**t may be provided to the after collection, but before: ● the **Participant,** its **Processors**, or any **Third Parties** make use of the **Sensitive Personal Information**, when the purposes of such use are not related or compatible to the purposes for which the information was collected; and ● **Sensitive Personal Information** is disclosed or distributed to **Third Parties**, other than **Processors** (e.g., agents, business associates, service providers, vendors).

Data Privacy Framework Principles: II.2.c Enterprise Practices Assessment Criteria 11	If the **Participant** identifies an applicable qualification to the provision of obtaining consent, TRUSTe must verify whether the applicable qualification is justified, or when 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 principle. If the **Participant** receives **Sensitive Personal Information** from a **Third Party** the **Third Party** has identified as sensitive, the **Participant** must treat it as sensitive. An organization is not required to obtain affirmative **Express 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 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 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 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 for subsequent uses or disclosures of **Sensitive Personal Information**. Gaps and Remediation: If affirmative **Express Consent** (opt-in) is not obtained and the **Participant** does not identify an acceptable qualification, TRUSTe must inform the **Participant** that a mechanism to obtain **Express Consent** must be provided and 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 principle.

ACCOUNTABILITY FOR ONWARD TRANSFER The purpose of the Accountability for Onward Transfer Principle is to ensure that the recipient of transferred information will protect the information in accordance with the Principles described herein. An organization must enter into a contract with any **Controller** or **Processor**, unless the organization is a **Controller** that is transferring personal information to another **Controller** within a controlled group of entities. The requisite contractual requirements will differ depending on if the recipient party is a **Controller** or **Processor**. Refer to the Data Privacy Framework Assessment Criteria, below, for the requirements.	
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. Data Privacy Framework Principles: II.3.a APEC CBPR Requirement: 10-13 Enterprise Practices Assessment Criteria: 9	**22. Onward Transfer to Third Parties** Requirement: To transfer **Personal Information** to a **Third Party**, the **Participant** must comply with the Notice and Choice Principles outlined above. The **Participant** must offer the **Individual** the opportunity to choose (opt out) whether their Personal Information is to be: ● disclosed to a Third Party (other than a third party that is acting as a Processor to perform task(s) on behalf of and under the instructions of the Participant); or ● disclosed for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the Individual. Evaluation: For those transfers that do not require the **Individual** be given the opportunity to opt-out TRUSTe must require the **Participant** to identify: ● each type of data disclosed or transferred; ● the corresponding stated purpose of the collection, use, or disclosure for each type of disclosed data; and ● the manner in which the disclosure is compatible with the identified purpose (e.g., order fulfillment etc.). Gaps and Remediation: If this information is not provided,TRUSTe must inform the **Participant** that: each type of data disclosed or transferred; the corresponding stated purpose of the collection, use, or

	disclosure for each type of disclosed data; and the manner in which the disclosure is compatible with the the identified purpose (e.g., order fulfillment etc.) needs to be identified.
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. Data Privacy Framework Principles: II.3.a APEC CBPR Requirement: 46	**23. Contracts with Controllers** Requirement: The **Participant** must have contracts in place with **Controllers** pertaining to **Personal Information** that is transferred to them to ensure that the obligations to the **Individual** undertaken at the time of collection will be met. Application of Access and the Onward Transfer Principle need not be provided for "occasional employment-related operational needs (e.g., booking of a flight, hotel room, or insurance coverage) of the Data Privacy Framework organization . . . [if] the Data Privacy Framework organization has complied with the Notice and Choice Principles." Evaluation: TRUSTe must verify the existence of the agreement(s) described. TRUSTe must verify that the **Participant** has entered into a contract with any **Controllers** the **Participant** transfers **Personal Information** to. Gaps and Remediation: If the **Participant** does not have contracts in place, TRUSTe must inform the **Participant** that implementation of a contract with **Controllers** to which **Personal Information** is transferred to is required for compliance with this principle.
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. Data Privacy Framework Principles: II.3.a	**24. Establish and Maintain Contracts with Controllers** Requirement: Contracts with **Controller(s**) to which **Personal Information** is transferred to must require the following: ● the **Processing** of **Personal Information** to be limited to the purposes identified in the contract and consistent with the notice delivered and consent provided by the **Individual;** ● the **Controller** to notify the **Participant** if it determines it can no longer meet its requirements and to cease **Processing** or takes other reasonable and appropriate steps to remediate; and ● the **Controller** to provide the same protections as required under the Data Privacy Framework Principles. The contract is not required to include:

	● the requirement that the **Third-Party Controller** be a Data Privacy Framework organization; or ● that the **Third Party** has an independent recourse mechanism, if it makes available an equivalent mechanism. When **Personal Information** is transferred between two **Controller**s within a controlled group of corporations or entities, a contract is not always required—an organization can base transfers on other instruments, such as Binding Corporate Rules. Evaluation: TRUSTe must require the **Participant** to provide a copy of the template contract provision(s) it uses to ensure that: ● the **Controller** processes **Personal Information** in accordance with the purposes outlined in the contract and consistent with the notice delivered and consent provided by the **Individual;** ● the **Controller** provides the same protections as is required under the Data Privacy Framework Principles; and ● the **Controller** notifies the **Participant** if it makes the determination that it can no longer meet its requirements, and cease **Processing** or takes other reasonable and appropriate steps to remediate. Gaps and Remediation: TRUSTe must inform the **Participant** that all the contractual requirements described herein are required for compliance with this principle if the **Participant** has not included all the required provisions.
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.	**25. Contracts with Processors** Requirement: The **Participant** must have contracts in place with **Processors** (e.g., agents, business associates, service providers, vendors) pertaining to **Personal Information** they process on the Participant's behalf to ensure the Participant's obligations to the **Individual** undertaken at the time of collection will be met. Application of Access and the Onward Transfer Principle need not be provided for "occasional employment-related operational needs (e.g., booking of a flight, hotel room, or insurance coverage)

Data Privacy Framework Principles: II.3.b.ii APEC CBPR Requirement: 46	of the Data Privacy Framework organization . . . [if] the Data Privacy Framework organization has complied with the Notice and Choice Principles." 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**. Gaps and Remediation: If the **Participant** does not have contracts in place, TRUSTe must inform the **Participant** that implementation of a contract with **Processors** is required for compliance with this principle.
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. Data Privacy Framework Principles: II.3.b.i-vi	**26. Establish and Maintain Contracts with Processors** Requirement: Contracts in place with **Processor(s)** (e.g., agents, business associates, service providers, or vendors) must require the following: ● the **Processor** to process **Personal Information** in accordance with the **Controller's** instruction; ● the **Processor** to provide the same level of privacy protections as required by the Principles; ● the **Processor** to provide appropriate technical and organizational measures to protect **Personal Information** from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access; ● the **Processor** to understand when (and if) onward transfer (e.g., use of sub-processors) is allowed; ● the **Processor** to take into account the nature of the **Processing**, assists the **Controller** in responding to **Individuals** exercising their rights under the Principles (e.g., requiring **Processors** to respond to the **Controller's** request for information needed to respond to an access request); ● the **Processor** to notify the **Controller** if the **Processor** determines it can longer meet its requirements; and ● the **Processor** to, upon notice of unauthorized **Processing**, take reasonable and appropriate steps to stop and remediate unauthorized **Processing**.

	Evaluation: TRUSTe must require the **Participant** to provide a copy of the template contract provision(s) it uses to ensure that the **Processor** (e.g., agent, business associates, service provider, vendor): ● processes **Personal Information** in accordance with the **Participant's** instructions; ● provides at least the same level of privacy protections as is required by the principles; ● provides appropriate technical and organizational measures to protect **Personal Information** against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; ● assists the **Participant**, as instructed, in responding to individuals exercising their rights under the Principles; ● notifies the **Participant** if the **Processor** makes the determination that it can no longer meet its requirements; and ● upon notice of unauthorized **Processing**, takes reasonable and appropriate steps to stop and remediate any unauthorized **Processing**. Gaps and Remediation: TRUSTe must inform the **Participant** that all the contractual requirements described herein are required for compliance with this principle if the **Participant** has not included all the required provisions.
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. Data Privacy Framework Principles: II.3.b.ii Enterprise Practices Assessment Criteria 7	**27. Evaluate Processors** Requirement: The **Participant** must take steps to assess the practices of its **Processors** (e.g., agents, business associates, service providers, or vendors) to ensure those practices align with the **Participant's** obligations under the Data Privacy Framework Principles. Evaluation: TRUSTe must verify that the **Participant** has assessed whether the **Processor** provides the same level of protection as is required by the Principles. Gaps and Remediation: If the **Participant** does not take steps or have a process in place to assess its **Processors**, TRUSTe must inform the **Participant** that it must ascertain whether its **Processors** provide at least the same level of privacy protection as is required by the Principles.

SECURITY The purpose of the Security Principle is to ensure that when **Individuals** provide their **Personal Information** to an organization, the organization will implement reasonable and appropriate safeguards to prevent the **Personal Information** from loss, misuse and unauthorized access, disclosure, alteration and destruction. 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.	
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. Data Privacy Framework Principles: II.4.a APEC CBPR Requirement: 27 Enterprise Practices Assessment Criteria 22	**28. Security of Processing** Requirement: The **Participant** must implement 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.

	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, which may include: ● authentication and access control (e.g., password protections); ● encryption; ● boundary protection (e.g., firewalls, intrusion detection); ● audit logging; or ● monitoring (e.g., external and internal audits, vulnerability scans). 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 principle.
TrustArc P&DG Standard: *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. Data Privacy Framework Principles: II.4.a APEC CBPR Requirement: 28 Enterprise Practices Assessment Criteria 22	**29. Proportional Safeguards** Requirement: The safeguards that are in place must be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held. Evaluation: TRUSTe must verify that these safeguards are proportional to the risks identified. Gaps and Remediation: If the safeguards in place are not proportional to the identified risks, TRUSTe must inform the **Participant** that reasonable administrative, technical, and physical safeguards, suitable to the **Participant's** size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a **Third Party**) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access must be implemented.
TrustArc P&DG Standard: *Security:* Protect data from loss, misuse, and unauthorized access,	**30. Awareness and Training** Requirement: The **Participant** must make its employees aware of the importance of maintaining the security of **Personal Information** (e.g., through regular training and oversight).

disclosure, alteration, or destruction. Data Privacy Framework Principles: II.4.a and III.7.c APEC CBPR Requirement: 29 Enterprise Practices Assessment Criteria: 28	Evaluation: TRUSTe must verify that the **Participant's** employees are aware of the importance of, and obligations respecting, maintaining the 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 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 Principle.

DATA INTEGRITY AND PURPOSE LIMITATION The purpose of the Data Integrity and Purpose Limitation Principle is to ensure that **Personal Information** is reliable and accurate for as long as an organization retains the information. This includes collecting **Personal Information** by lawful and fair means and as in accordance with the organization's **Privacy Notice**, verifying that **Personal Information** is up to date, and establishing an information retention policy. Refer to the Data Privacy Framework Assessment Criteria, below, for the requirements.	
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. Data Privacy Framework Principles: III.8.a.i.2 APEC CBPR Requirement: 7 Enterprise Practices Assessment Criteria: 5	**31. Lawfulness of Processing** Requirement: The **Participant** must collect **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.** 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 of such **Personal Information** and that it is collecting information by fair means, without deception. Gaps and Remediation: If the **Participant** is unable to certify this, TRUSTe must inform that **Participant** that lawful and fair procedures are required for compliance with this principle.
TrustArc P&DG Standard: *Use, Retention, and Disposal:* Ensure data is used only as legally permissible and solely for	**32. 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**

purposes that are relevant to and compatible with the purposes for which it was collected. Data Privacy Framework Principles: II.5.a APEC CBPR Requirement: 8 Enterprise Practices Assessment Criteria: 3	**Privacy Notice** and/or in the 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 Notice(s)** 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** 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: *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.	**33. 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** which 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;

Data Privacy Framework Principles: II.5.a APEC CBPR Requirement: 6 Enterprise Practices Assessment Criteria: 1	• 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 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 Integrity and Quality:* Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use. Data Privacy Framework Principles: II.5.a APEC CBPR Requirement: 21 Enterprise Practices Assessment Criteria: 21	**34. 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 principle.
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. Data Privacy Framework Principles: II.5.b Enterprise Practices Assessment Criteria: 6	**35. 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 defined retention requirements such as those defined in the **Participant's** privacy policies. Gaps and Remediation: If the **Participant** does not have a defined retention period 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 Principle.

ACCESS

The purpose of the Access Principle is to allow **Individuals** to verify the accuracy of information held about them. In particular, the Access Principle requires organizations to provide confirmation to **Individuals** of whether or not they process the **Individual's Personal Information**, and to provide access to **Individuals** to verify the information and the lawfulness of the **Processing**. If an **Individual** discovers that information is incorrect or processed in violation of the Principles, the organization must correct, amend, or delete the **Personal Information**.The Access Principle is not absolute and is subject to exceptions. Refer to the Data Privacy Framework Assessment Criteria, below, for a list of exceptions.

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. Data Privacy Framework Principles: III.8.a.i.1 and III.8.f.i APEC CBPR Requirement: 36 Enterprise Practices Assessment Criteria: 16	**36. Right to Access** Requirement: Upon request, the **Participant** must provide confirmation of whether or not **Personal Information** has been collected or held about the requesting **Individual.** The **Participant** must grant access to any **Individual**, to **Personal Information** collected or gathered about that **Individual**, upon receipt of sufficient information confirming the **Individual's** identity. The **Participant's** processes or mechanisms for access by **Individuals** to **Personal Information** 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 **Personal Information** must be provided to **Individuals** in an easily comprehensible way. Under the Data Privacy Framework, access may be denied or limited under the following circumstances as outlined in Supplemental Principle 8 (Access): ● 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 organization’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—include 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 organization. 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, or a third party Processor,** stores or retains for a period of time, the **Personal Information** it collects, uses, and discloses. 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.

	Evaluation: TRUSTe must verify that the **Participant** has procedures in place to respond to such requests. Gaps and Remediation: If the **Participant** does not have procedures for this, TRUSTe must inform the **Participant** that the existence of written procedures to respond to such requests is required for compliance with this principle.
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. Data Privacy Framework Principles: III.8.a.i.2 APEC CBPR Requirement: 38 Enterprise Practices Assessment Criteria: 17	**37. Right to Rectification** Requirement: The **Participant** must have available, operational, and understandable policies to enable **Individuals** to: ● challenge the accuracy and lawfulness of processing of their information, and to have it rectified, completed, amended, and/or deleted; ● 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. If an **Individual** demonstrates that **Personal Information** about them is incomplete or incorrect, the **Participant** must make the requested correction, addition, or where appropriate, deletion. The **Participant** must make such corrections or deletions within a reasonable time frame following an **Individual's** request for correction or deletion. 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. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to **Individuals** that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests.

	Evaluation: TRUSTe must verify that such policies are available, operational, and understandable in the EU, Switzerland, and/or UK. 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 principle. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.

RECOURSE, ENFORCEMENT, AND LIABILITY

The purpose of the Recourse, Enforcement, and Liability Principle is to ensure an organization's compliance with the Principles and that **Individuals** affected by an organization's non-compliance with the Principles have recourse. Accountability, and having mechanisms in place to hold organizations accountable to the Principles, is the cornerstone of any effective framework. The Principle requires that organizations have mechanisms in place to respond to and receive complaints. Refer to the Data Privacy Framework Assessment Criteria, below, for the requirements.

TrustArc P&DG Framework and External Regulatory Standard Mapping	Assessment Criteria
TrustArc P&DG Standard: *Processes:* Establish, manage, measure, and continually improve processes for PIAs, vendor assessments, incident management and breach notification, complaint handling, and individual rights management. Data Privacy Framework Principles: II.7.a.i CBPR PR 41	**38. Dispute Resolution Mechanism** Requirement: The **Participant** must have a mechanism in place to receive and respond to complaints or questions regarding its compliance with the Principles. Evaluation: TRUSTe must verify that the **Participant** has a mechanism in place to receive complaints or questions about the **Participant's** compliance with the Principles. Gaps and Remediation: If the **Participant** does not have a mechanism in place, TRUSTe must inform the **Participant** that implementation of such mechanism is required for compliance with this Principle.

TrustArc P&DG Standard: *Processes:* Establish, manage, measure, and continually improve processes for PIAs, vendor assessments, incident management and breach notification, complaint handling, and individual rights management. Data Privacy Framework Principles: II.7.a.i	**39. Complaints Handling Process** Requirement: The **Participant's** procedure for responding to **Individuals'** complaints or questions must require that an **Individual** receive a response within no more than 45 days of receiving the **Individual's** complaint. Evaluation: TRUSTe must verify that the **Participant** has procedures in place to ensure **Individuals** receive a response to their complaints within 45 days of receiving a complaint. Gaps and Remediation: If the **Participant's** complaint handling procedure does not require that an **Individual** receive a response within 45 days of receiving the **Individual's** complaint, TRUSTe must inform the **Participant** that implementation of such procedures is required for compliance with this Principle.

HUMAN RESOURCES DATA

The purpose of the Human Resources Data Supplemental Principle is to highlight specific Data Privacy Framework Principles, in addition to the criteria above, relating to the transfer of Human Resources Data. The supplemental principle ensures that when an organization in the EU transfers **Personal Information** about its employees to an organization in the United States, the transferred employee **Personal Information** is used and disclosed in ways that are consistent with the employees' expectations. Human Resources data may only be transferred by an EU company to the U.S. if the receiving company has a valid Data Privacy Framework certification for Human Resources Data on the U.S. Department of Commerce's Data Privacy Framework website.

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. Data Privacy Framework Principles: III.9.b.iii	**40. Employee Privacy Preferences** Requirement: The **Participant** must have mechanisms in place to honor employee privacy preferences. Notice and Choice need not be provided for a period necessary to avoid prejudicing the ability of the organization to make promotions, appointments, or other similar employment decisions. Evaluation: TRUSTe must verify that the **Participant** has reasonable mechanisms in place to honor employee privacy preferences—for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand. Gaps and Remediation: If TRUSTe determines the **Participant** does not have reasonable mechanisms in place to honor employee privacy preferences, TRUSTe must inform the **Participant** that providing reasonable mechanisms to accommodate employee privacy preferences is required for compliance with this principle.

PHARMACEUTICAL AND MEDICAL PRODUCTS The purpose of the Pharmaceutical and Medical Products Supplemental Principle is to highlight specific requirements under Data Privacy Framework relating to pharmaceutical and medical products. The supplemental principles ensures that when an organization in the EU transfers **Personal Information** developed in medical or pharmaceutical research activities to the United States, the transferred **Personal Information** is used and disclosed in ways that are consistent with an **Individual's** expectations.	
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. Data Privacy Framework Principles: III.14.a.i	**41. Data Anonymization** Requirement: The **Participant** must anonymize**,** where appropriate, **Personal Information** that is used for medical product and pharmaceutical research purposes. Data Privacy Framework Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles do not apply to a Pharmaceutical organization's product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. Evaluation: TRUSTe must verify that the **Participant** has mechanisms in place to anonymize **Personal Information** when appropriate. TRUSTe must require the **Participant** to provide a description of how the **Participant** determines when it is appropriate to anonymize **Personal Information**. TRUSTe must require the **Participant** to certify that it adequately de-identifies **Personal Information**.

	Gaps and Remediation: If the **Participant** does not show that **Personal Information** is appropriately anonymized, TRUSTe must inform the **Participant** that policies must be developed for determining when **Personal Information** should be anonymized, and adequate anonymization methods must be used so that **Personal Information** cannot be re-identified. Such requirements are required for compliance with this Principle.
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. Data Privacy Framework Principles: III.14.b.i	**42. Transfer of Personal Information for Research Studies** Requirement: The **Participant** may rely on the Data Privacy Framework for the transfer of **Personal Information** that was developed in specific medical or pharmaceutical research studies for use in a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. The **Participant** must verify **Individuals** were provided notice and the opportunity to consent to having their **Personal Information** used for future scientific research studies at the time the **Individual** consented to participating in the initial study. Evaluation: TRUSTe must verify that the **Participant** has policies and processes in place to verify notice and an opportunity to consent has been provided to **Individuals** about the use of their **Personal Information** in future scientific research studies. Gaps and Remediation: If the **Participant** does not have policies or processes in place to verify **Individuals** were provided notice and an opportunity to consent to having their **Personal Information** use for future scientific research studies, TRUSTe must inform the **Participant** that such verification is required for compliance with this Principle.
TrustArc P&DG Standard: *Transparency:* Inform individuals about the ways in which data about them are processed and how to	**43. Future Uses or Unanticipated Research Activities.** Requirement: The **Participant** must provide **Individuals** notice at the time **Personal Information** is collected of a) potential future specific uses (i.e., periodic follow-up, related studies, or marketing), and b) potential future unanticipated medical and pharmaceutical research activities.

exercise their data-related rights. Data Privacy Framework Principles: III.14.b.ii	Evaluation: TRUSTe must verify that the **Participant** provides notice to I**ndividuals** about the potential future specific uses and potential future unanticipated medical and pharmaceutical research activities. Gaps and Remediation: TRUSTe must inform the **Participant** that if the **Personal Information** will be used for purposes that are not consistent with the general research purposes for which it was originally collected, or to which the **Individual** had subsequently consent, the **Participant** must obtain new consent. If the **Participant** does not provide notice to **Individuals** about potential future uses or unanticipated research activities, TRUSTe must inform the **Participant** that notice is required for compliance with this Principle.
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. Data Privacy Framework Principles: III.14.b.ii	**44. Consent for Future Research Activities** Requirement: The Participant must obtain new consent if **Personal Information** will be used for future medical and pharmaceutical research activities that are not consistent with the general research purpose(s) for which it was originally collected, or to which the **Individual** had subsequently consented. Evaluation: If an **Individual's Personal Information** is used for for future medical and pharmaceutical research activities purpose that are not consistent with the purpose(s) for which it was originally collected or for which the **Individual** had subsequently consented, TRUSTe must verify that the **Participant** has procedures in place to ensure **Individuals** receive new notice of such uses. Gaps and Remediation: If the **Participant** does not provide a policy that describes the procedures in place, TRUSTe must require the **Participant** to certify that it provides notice to **Individuals** if the **Participant** wants to use **Personal Information** for future medical and pharmaceutical research activities that are inconsistent with the purpose(s) for which it was originally collected, or to which the **Individual** had subsequently consented.

	If the **Participant** wants to use **Personal Information** for future medical and pharmaceutical research activities that are inconsistent with the purpose(s) for which it was originally collected or for which the **Individual** had subsequently consented, and does not have procedures in place to obtain new consent from the **Individual**, TRUSTe must inform the **Participant** that it must have a process in place to obtain new consent.
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. Data Privacy Framework Principles: III.14.e.i	**45. Clinical Trials** Requirement: The **Participant** must provide notice to Individuals at the time the **Individual** agrees to participate in a clinical trial if the **Participant** intends to continue to process the **Individual's** data after the **Individual** has withdrawn from the clinical trial. Evaluation: If **Participant's** organization processes data after an **Individual** has withdrawn from a clinical trial, TRUSTe must verify that the **Participant** provides notice to **Individuals**, at the time he or she agrees to participate in a clinical trial, that any personal data collected previous to withdrawal from the clinical trial will be processed along with other data collected as part of the clinical trial. Gaps and Remediation: If the **Participant's** organization does not identify an applicable qualification, TRUSTe must notify the **Participant** that such information is required for compliance with this Principle and must be included in their **Privacy Notice**. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.

III. DEFINITIONS

“Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

“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 data” and “personal information” are data about an identified or identifiable **Individual** that are within the scope of the GDPR, received by an organization in the United States from the EU, and recorded in any form.

“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.

“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 is not directly affiliated with the **Participant**; or, if affiliated with the **Participant**, such affiliation is not reasonably known to the **Individual**.