Data Collection Certification Assessment Criteria

TABLE OF CONTENTS

Data Collection Certification Assessment Criteria

I. INTRODUCTION

TRUSTe LLC ("TRUSTe"), a subsidiary of TrustArc Inc ("TrustArc"), 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, Federal Trade Commission's Self-Regulatory Guidelines on OBA. and self-regulatory industry frameworks including the Digital Advertising Alliance's (DAA) Self-Regulatory Principles, the European DAA Online Behavioral Advertising Principles, and the 2018 NAI Code of Conduct.

The TRUSTe Data Collection Certification is designed to enable organizations, who help in the optimization or serving of an online advertisement to demonstrate that their privacy and data governance practices for the collection and use of data for **Online Behavioral Advertising** comply with the standards outlined in these Assessment Criteria. The 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 eleven of TrustArc's Framework BUILD, IMPLEMENT, and DEMONSTRATE Standards: including:

IMPLEMENT Standards

- Data Necessity:

Data Collection Certification Assessment Criteria

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

DEMONSTRATE Standards
- Reporting and Certification

BUILD Standards
- Resource Allocation
- Processes

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.

Data Collection Certification Assessment Criteria

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

*Defined terms appear in **bold***.

Data Collection Certification Assessment Criteria

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. 2 Total Requirements 2 Required 0 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT 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.	**1. Collection Limitation** Requirement: The **Participant** must only collect data where such data is limited to the specific data reasonably useful for the purpose for which it was collected and in accordance with the **Participant's Privacy Notice** and/or in-ad notice. Evaluation: Using the above, TRUSTe will verify that the **Participant** limits the amount and type of data collected to that which is relevant to fulfill the stated purposes. Gaps and Remediation: If the **Participant** indicates that it does not limit the amount of data collected to what is relevant to the identified collection purpose, TRUSTe must inform the **Participant** that it must limit the use of collected data to those uses that are relevant to fulfilling the purpose(s) for which it is collected.

Data Collection Certification Assessment Criteria

	GDPR Article 5(1)(c)	
Required	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct I.D, I.E. DAA Self-Regulatory Principles for Online Behavioral Advertising IV.C.1 and IV.C.3	**2. Data Anonymization** Requirement: The **Participant** must leverage anonymization, **De-identification**, **Pseudonymizatio**n, coding, or similar mechanisms to mitigate data storage-related risks. These mechanisms and techniques must not enable the **Participan**t or a **Third Party** to reconstruct or combine the data in way that enables re-identification of the **Individual**. This requirement shall not pertain to **Device-Identifiable Information**. Evaluation: Where the **Participant** indicates that data does not need to be retained as required in Assessment Criteria 8, or no longer needs to be retained in an identifiable form, TRUSTe will verify that the **Participant** has processes in place to mitigate data storage-related risks through leveraging anonymization, D**e-identification**, **Pseudonymization**, coding, or similar mechanisms that do not enable the **Participant** or a **Third Party** to reconstruct the data to re-identify the **Individual**. 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 and that such mechanism must not enable the **Participant** or a **Third Party** to reconstruct the data to re-identify the **Individual.**

Data Collection Certification Assessment Criteria

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. 6 Total Requirements 4 Required 2 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT 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. DAA Self-Regulatory Principles for Online Behavioral Advertising V. and VI.B DAA Self-Regulatory Principles for Multi-Site Data II	**3. Purpose Limitation** Requirement: The **Participant** must handle all collected data in accordance with the posted **Privacy Notice** in effect at the time of collection unless the **Individual** otherwise has given **Express Consent** for specific uses beyond the scope of the **Privacy Notice**. The **Participant** must only use or allow the use of collected data for the following purposes: ● **Online Behavioral Advertising**; ● operations and systems management including: ○ intellectual property protection; ○ compliance, public purpose, and consumer safety; ○ authentication, verification, fraud prevention, and security; ○ billing or product or service fulfillment; or ○ **Ad Reporting** or **Ad Delivery**; ● market research or product development including the analysis of the characteristics of a group of consumers or market, and product performance

Data Collection Certification Assessment Criteria

	DAA Application of Self-Regulatory Principles to the Mobile Environment VII & VIII European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the European Self Regulatory Programme on OBA 2.2.1 2018 NAI Code of Conduct II.D.2 and II.D.3	to improve existing or new products using de-identified data that has been de-identified in such a way that an **Individual** cannot be re-identified; and ● in accordance with the **Participant's Privacy Notice** and/or in-ad notice unless the **Individual** has been provided notice and has given **Express Consent** for specific uses beyond the scope of the **Privacy Notice**. Collected data must not be used to or be made available to **Third Parties** for the following purposes: ● credit eligibility; ● employment eligibility; ● insurance eligibility, underwriting, and pricing; ● health care treatment eligibility; ● providing targeted marketing to children under age 13; and ● targeting or marketing to children under age 18 if such advertising contains content not reasonably appropriate for this age group. An identifier issued for the specific purpose of communicating, honoring, reading, or otherwise managing privacy preferences must not be used for any other purpose. The **Participant** must not collect, use, or make available to **Third Parties**, except for **Processors**, data containing **Contact Information** or **Sensitive Information** unless the **Individual** has been provided notice and given **Express Consent**. Evaluation: TRUSTe will verify that the **Participant** handles all collected data in accordance with the posted **Privacy Notice** in effect at the time of collection and in accordance with the permissible purposes. Gap and Remediation: If the **Participant** cannot verify that it handles collected data for permissible purposes and/or in accordance with the **Privacy Notice**, TRUSTe must inform the **Participant** that the collected data must only be used for permissible

Data Collection Certification Assessment Criteria

		purposes and in accordance with the **Privacy Notice** in effect at the time of collection, unless the **Individual** has given **Express Consent** for specific uses beyond the scope of the **Privacy Notice**.
Conditional	**TrustArc P&DG IMPLEMENT 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. Children's Online Privacy Protection Rule §312.5 Parental consent (c)(7)	**4. Children's Information** Requirement: On web sites or apps directed towards children under age 13 as allowed by the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, et seq., the **Participant** may: ● maintain or analyze the functioning of the website or online service; ● perform network communications; ● serve contextual advertising on the website or online service or cap the frequency of advertising; ● protect the security or integrity of the user, website, or online service; and ● ensure legal or regulatory compliance. Evaluation: TRUSTe will verify that the **Participant** processes children's data only for the listed purposes. Gap and Remediation: If the **Participant** cannot demonstrate that it only processes the children's data for the listed purposes, TRUSTe must inform the **Participant** that it can only process children's data in accordance with the listed purposes for compliance with this requirement.
Required	**TrustArc P&DG IMPLEMENT 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	**5. Data Retention** Requirement: The **Participant** will retain data collected for **Online Behavioral Advertising**: ● For as long as commercially useful to carry out its business purpose or until the **Individua**l expresses an opt-out preference, but no longer than 24 months in an identifiable form; or as required by law.

Data Collection Certification Assessment Criteria

	purposes for which it was collected. 2018 NAI Code of Conduct II.F.4 DAA Self-Regulatory Principles for Online Behavioral Advertising IV.B European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.1.2	• For data that has been de-identified so the data cannot be used to re-identify the **Individual**, for as long as commercially useful to carry out its business purpose. Evaluation: TRUSTe will verify that the **Participant** retains data collected for **Online Behavioral Advertising**: • For as long as commercially useful to carry out its business purpose or until an **Individual** expresses an opt-out preference, but no longer than 24 months in an identifiable form, including individually-identifiable and device-identifiable form; or as required by law. • For data that has been de-identified so the data cannot be used to re-identify the **Individual**, for as long as commercially useful to carry out its business purpose. Gap and Remediation: If the **Participant** cannot verify this, TRUSTe must inform the **Participant** that data collected for **Online Behavioral Advertising** can only be retained: • For as long as commercially useful to carry out its business purpose or until an **Individua**l expresses an opt-out preference, but no longer than 24 months in an identifiable form; or as required by law. • For data that has been de-identified so the data cannot be used to re-identify the **Individual,** for as long as commercially useful to carry out its business purpose.
Required	**TrustArc P&DG IMPLEMENT Standard:** *Use, Retention, and Disposal:* Ensure data is used only as legally	**6. Lawfulness of Processing** Requirement: The **Participant** must process collected data (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

Data Collection Certification Assessment Criteria

	permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected. GDPR Articles 5(1)(a) and 6(1).	data. Examples of lawful means include, but are not limited to: consent, a contract with the **Individual,** a legal obligation, for the health and safety of the individual, in the public interest, and for 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 data 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.
Conditional	**TrustArc P&DG IMPLEMENT 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. DAA Self-Regulatory Principles for Online Behavioral Advertising IV.C.3	**7. Third Party Data Sources** Requirement: All data sources that the **Participant** uses must contain appropriate agreements showing that all data received was obtained under legitimate means and limitations regarding the collection, use, and onward transfer of the data are satisfied. Evaluation: TRUSTe will verify that the **Participant** has processes in place to ensure that all data sources that the **Participant** uses contain appropriate agreements. Gap and Remediation: If the **Participant** does not have processes in place to ensure that all data sources that the **Participant** uses contain appropriate agreements showing that all data received was obtained under legitimate means and limitations regarding the collection, use, and onward transfer of the data are satisfied, TRUSTe must inform the **Participant** that a process to ensure this is required for compliance with this requirement.

Data Collection Certification Assessment Criteria

	DAA Application of Self-Regulatory Principles to the Mobile Environment IV.B.2 European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.9 and 2.10 2018 NAI Code of Conduct II.F.2	
Required	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct II.F.4	**8. Define and Communicate Retention Periods** Requirement: The **Participant** must define and communicate retention periods for retaining data collected for **Online Behavioral Advertising** (e.g., information retention policy, retention schedules, or retention requirements). The defined retention period shall not exceed 24 months or as required by law per Assessment Criterion 5. 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.

Data Collection Certification Assessment Criteria

	DAA Self-Regulatory Principles for Online Behavioral Advertising IV.B European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the European Self Regulatory Programme on OBA 2.1.2 GDPR Articles 5(1)(e), 13-14, and 30(1)(f)	Gaps and Remediation: If the **Participant** does not have defined retention periods in place for data collected for **Online Behavioral Advertising** and has not communicated the retention periods, TRUSTe must inform the **Participant** that the implementation of defined information retention periods and communication of such are required for compliance with this requirement.

Data Collection Certification Assessment Criteria

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. 4 Total Requirements 2 Required 2 Conditional		
Type	**TrustArc P&DG Framework and ExternalRegulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT 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. European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.1.1 (3)	**9. Evaluate Processors** Requirement: The **Participant** must have a process in place to evaluate the privacy and security practices of its **Processors** (e.g., agents, business associates, service providers, or vendors) to ensure the **Processors** have 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 to evaluate the privacy and security practices of its **Processors** that comply with the controls and standards herein and with applicable laws. Gaps and Remediation: If the **Participant** does not have such a process in place, TRUSTe must inform the **Participant** that it must have a process in place to ascertain whether its **Processors** have effective safeguards and controls in place that comply with the controls and standards herein and with applicable laws.

Data Collection Certification Assessment Criteria

	2018 NAI Code of Conduct II.E.1 GDPR Article 28.1 ISO 27001 8.2 Information Security Risk Assessment	
Required	**TrustArc P&DG IMPLEMENT 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. DAA Self-Regulatory Principles for Online Behavioral Advertising IV.C.3 2018 NAI Code of Conduct II.E.1 European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the	**10. Contracts with Processors** Requirement: The **Participant** must have appropriate contracts in place with **Processors** (e.g., agents, business associates, service providers, vendors) pertaining to data they process on the **Participant's** behalf, which ● limit the processing of data to be only in accordance with instructions from the **Participant**; ● require the **Processors** to abide by the rights and obligations attached to the data by the **Participant** regarding the security, confidentiality, integrity, use, and disclosure of the data; and ● ensures the **Participant's** obligations to the **Individual** undertaken by the **Participant** will be met and that appropriate data protections are in place. Evaluation: TRUSTe must verify the existence of each type of agreement described. TRUSTe must verify that the **Participant** has entered into contracts with **Processors** to ensure the data protections appropriate to the nature of the relationship with the **Processors** are in place. Gaps and Remediation: If the **Participant** does not have appropriate contracts in place, TRUSTe must inform the **Participant** that implementation of contracts with **Processors** are required for compliance with this requirement.

Data Collection Certification Assessment Criteria

	European Self Regulatory Programme on OBA 2.9 and 2.10	
Conditional	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct II.B.3-5 DAA Application of Self-Regulatory Principles to the Mobile Environment IV.B.1	**11. First Parties** Requirement: Where the **Participant** has a direct relationship with its **First Party** partners, the **Participant** must have processes in place to require its **First Party** partners to: ● include disclosures in the **First Party's Privacy Notice** listing the types of **Third Parties** that collect data through the **First Party's** application or website, including **Third Parties** that collect data about an **Individual's** online activities across multiple unaffiliated applications or websites, and how that data is used; and ● provide **Clear and Conspicuous** access to preference management tools where **Individuals** can exercise their preference, including withdrawing consent, regarding whether their data is collected and used for the purposes of **Online Behavioral Advertising**. Evaluation: TRUSTe must verify that, where the **Participant** has a direct relationship with its **First Party** partners, the **Participant** has processes in place to require its **First Party** partners to: ● include disclosures in the **First Party's Privacy Notice** listing the types of **Third Parties** that collect data through the **First Party's** application or website including **Third Parties** that collect data about an **Individual's** online activities across multiple unaffiliated applications or websites, and how that data is used; and ● provide **Clear and Conspicuous** access to preference management tools where **Individuals** can exercise their preference, including withdrawing consent, on whether their data is collected and used for the purposes of **Online Behavioral Advertising**

Data Collection Certification Assessment Criteria

		Gap and Remediation: If the **Participant** does not have the required processes in place, TRUSTe must inform the **Participant** that, to comply with this requirement, it must implement processes to ensure that its **First Party** partners: ● include disclosures in the **First Party's Privacy Notice** listing the types of **Third Parties** that collect data through the **First Party's** application or website including **Third Parties** that collect data about an **Individual's** online activities across multiple unaffiliated applications or websites, and how that data is used; and ● provide **Clear and Conspicuous** access to preference management tools where **Individuals** can exercise their preference, including withdrawing consent, on whether their data is collected and used for the purposes of **Online Behavioral Advertising**.
Conditional	**TrustArc P&DG IMPLEMENT 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. DAA Self-Regulatory Principles for Online Behavioral Advertising IV.C.2 - IV.C.4	**12. Contracts with Third Parties** Requirement: The **Participant** must have appropriate contracts in place with any **Third Party** or affiliated entity that the **Participant** discloses or otherwise transfers **Personal Information** to ensure that: ● if more than one **Ad Company** is involved in the ad chain, the **Participant**, if the **Participant** is not directly serving the ad to the **Individual**, will verify that the **Ad Company** directly involved provides enhanced notice and access to preference management tools; ● **Third Parties** or affiliated entities will not attempt to reconstruct de-identified data, and will use or disclose the anonymized data only for purposes of **Online Behavioral Advertising** or other uses as specified to **Individuals;** and ● **Third Parties** or affiliated entities who disclose anonymized data to other entities will take reasonable measures to ensure those entities receiving the data agree to the restrictions and conditions regarding the use of the data.

		● **Third Parties** or affiliated entities will not further share **Personal Information** received from the **Participant** with other **Third Parties,** and will limit any **Personal Information** that may be further shared with other **Third Parties** to **Derived Products**. Evaluation: TRUSTe must verify the existence of the contracts in place with **Third Parties** and/or affiliated entities that the **Participant** discloses or otherwise transfers **Personal Information** to and that the contracts contain the appropriate requirements. Gap and Remediation: If the **Participant** does not have appropriate contracts in place, TRUSTe must inform the **Participant** that, to comply with this requirement, it must have contracts in place with **Third Parties** or affiliated entities to ensure that: ● if more than one **Ad Company** is involved in the ad chain, the **Participant**, if the **Participant** is not directly serving the ad to the **Individual**, will verify that the **Ad Company** directly involved provides enhanced notice and access to preference management tools; ● **Third Parties** or affiliated entities will not attempt to reconstruct de-identified data and will use or disclose the anonymized data only for purposes of **Online Behavioral Advertising** or other uses as specified to **Individuals;** and ● **Third Parties** or affiliated entities who disclose anonymized data to other entities will take reasonable measures to ensure those entities receiving the data agree to the restrictions and conditions regarding the use of the data. ● **Third Parties** or affiliated entities will not further share **Personal Information** received from the **Participant** with other **Third Parties, and will** limit any **Personal Information** that may be further shared with other **Third Parties** to **Derived Products**.

Data Collection Certification Assessment Criteria

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. 8 Total Requirements 5 Required 3 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT 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.	**13. Choice for Online Behavioral Advertising** Requirement: The **Participant** must provide **Individuals** with the ability to exercise choice regarding the collection and use of their data for **Online Behavioral Advertising,** including by third parties with whom such data may be shared. Opt-out choice needs to be provided, consistent with Assessment Criterion 6, for: ● use of non-personal information or **Pseudonymous Data** for **Online Behavioral Advertising**; ● use of **Personal Information** to be merged with non-personal Information, including **Device-Identifiable Information**, on a going-forward basis for **Online Behavioral Advertising** purposes; and ● use of **Device-Identifiable Information** for **Online Behavioral Advertising**. **Express Consent** needs to be obtained for:

Data Collection Certification Assessment Criteria

	2018 NAI Code of Conduct II.C.1 and II.C. 2 DAA Self-Regulatory Principles for Online Behavioral Advertising III.A, and III.B.1 DAA Application of Self-Regulatory Principles to the Mobile Environment II.B.2 Application of the DAA Principles of Transparency and Control to Data Used Across Devices Control European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the European Self	• use of **Personal Information** merged with previously collected non-personal information, including **Device-Identifiable Information**; • use of **Precise Geo-location Data**; • use of **Contact Information** or **Sensitive Information**; and • **ISPs** and **Web Browser Providers** to collect and use data for **Online Behavioral Advertising** purposes Evaluation: TRUSTe must verify that the **Participant** provides **Individuals** with the ability to exercise choice regarding the collection and use of their data for **Online Behavioral Advertising,** including by third parties with whom such data may be shared. Gap and Remediation: If the **Participant** does not provide **Individuals** with the ability to exercise choice regarding the collection and use of their data for **Online Behavioral Advertising**, TRUSTe must inform the **Participant** that providing **Individuals** with choice regarding the collection and use of their **Personal Information** for **Online Behavioral Advertising** is required for compliance with this requirement.

	Regulatory Programme on OBA 2.2.2 and 2.8	
Conditional	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct II.C.1.f DAA Application of Self-Regulatory Principles to the Mobile Environment V	**14. Personal Directory Data** Requirement: **Personal Directory Data** will only be used for **Online Behavioral Advertising** if the **First Party** partner has obtained authorization through providing **Clear and Conspicuous** notice and obtaining **Express Consent** from the **Individual**. ● **Participant** must ensure its **First Party** partners have authorization from **Individuals** to authorize the **Participant** to collect **Personal Directory Data**. ● **Participant** must ensure the **First Parties** offer a mechanism for **Individuals** to withdraw consent for further collection and use of **Personal Directory Data**. Evaluation: TRUSTe must verify that the **Participant:** ● uses **Personal Directory Data** for **Online Behavioral Advertising** only if its **First Party** partners have obtained authorization through providing **Clear and Conspicuous** notice and obtaining **Express Consent** from the **Individual**; ● ensures its **First Party** partners have authorization from the **Individual** to authorize the **Participant** to collect **Personal Directory Data**; and ● ensure its **First Party** partners offer a mechanism for the **Individual** to withdraw consent for further collection and use of **Personal Directory Data**. Gap and Remediation: If the **Participant** cannot ensure that its **First Party** partners: ● obtain authorization through providing **Clear and Conspicuous** notice and obtaining **Express Consent** from the **Individual;** ● have authorization from the **Individual** to authorize the **Participant** to collect **Personal Directory Data**; and ● offer a mechanism for the Individual to withdraw consent for further collection and use of Personal Directory Data.

Data Collection Certification Assessment Criteria

		TRUSTe must inform the Participant that the above requirements must be met for compliance with this requirement.
Required	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct II.C.4	**15. Honoring Privacy Preferences** Requirement: The **Participant** must honor and maintain the **Individual's** selected preference in a persistent manner until the **Individual** changes that preference. A preference indicated through any industry recognized standardized choice platform (e.g. DAA, DAAC, EDAA, or NAI) or browser preference management tool, or communicated to the **Participant** by a **Third Party**, must be recognized as the Individual's express preference and honored per these requirements. Evaluation: TRUSTe must verify that the **Participant** honors and maintains the **Individual's** selected preference in a persistent manner until the **Individual** changes that preference. Gap and Remediation: If the **Participant** does not honor and maintain the **Individual's** selected preference, TRUSTe must inform the **Participant** that honoring and maintaining an **Individuals'** selected preferences in a persistent manner is required for compliance with this requirement.
Required	**TrustArc P&DG IMPLEMENT Standard:** *Choice and Consent:* Enable individuals to choose whether personal data about them is processed.	**16. Applicability of Privacy Preference** Requirement: An **Individual's** preference will be applied as broadly as possible across different technology platforms (e.g., mobile browser and apps where technically feasible, and in general accordance with user expectations).

	Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. 2018 NAI Code of Conduct II.C.5 European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the European Self Regulatory Programme on OBA 2.8	If a privacy preference is received, the **Participant** must no longer use the **Individual's** historical data and it must not collect any new data about an **Individual** for 48 hours after being made aware of the **Individual's** privacy preference. Evaluation: TRUSTe must verify that the **Participant** applies **Individuals'** preferences as broadly across different technology platforms; and that if a privacy preference is received, the **Participant** does not use an **Individual's** historical data and does not collect any new data about that **Individual** for 48 hours after being made aware of the **Individual's** privacy preference. Gap and Remediation: If the **Participant** does not apply **Individuals'** preferences as broadly as possible across different technologies, and/or the **Participant** uses the historical data or collects new data from **Individuals** within 48 hours of receiving a privacy preference, TRUSTe must inform the **Participant** that, for compliance with this requirement: ● **Individuals'** preferences must be applied as broadly as possible across different technology platforms (e.g., mobile browser and apps where technically feasible, and in general accordance with user expectations); and ● if a privacy preference is received, the **Participant** must not use the Individual's historical data and must not collect any new data about that **Individual** within 48 hours of being made aware of the **Individual's** privacy preference.
Conditional	**TrustArc P&DG IMPLEMENT Standard:** *Choice and Consent:* Enable individuals to choose whether	**17. Cross-Device Tracking** Requirement: When an **Individual** has exercised a preference pertaining to **Online Behavioral Advertising** through a browser or **Device**, the **Participant** must apply the **Individual's** preference to the browser or **Device** from which the preference was exercised and any browser and **Device** associated through **Cross-Device Tracking.**

	personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. 2018 NAI Code of Conduct II.C.3 Application of the DAA Principles of Transparency and Control to Data Used Across Devices Control	When such a preference is received**,** the **Participant** will no longer: ● collect data from the browser or **Device** where the **Individual** expressed their preference for **Online Behavioral Advertisin**g purposes; ● use the data on the browser and **Device** where the **Individual** expressed their preference, and any browser and **Device** associated through **Cross-Device Tracking** for **Online Behavioral Advertising** purposes; and ● provide or serve **Online Behavioral Advertising** on the browser and **Device** where the **Individual** expressed their preference, and any browser and **Device** associated through **Cross-Device Tracking**. Evaluation: TRUSTe must verify that—when an **Individual** has exercised a preference pertaining to **Online Behavioral Advertising** through a browser or **Device**—the **Participant** applies the **Individual's** preference to the browser or **Device** from which the preference was exercised and any browser and **Device** associated through **Cross-Device Tracking.** Gap and Remediation: If the **Participant** cannot verify that it applies an **Individual's** preference to the browser or device from which the preference was exercised, TRUSTe must inform the **Participant** that—when an **Individual** exercises a preference pertaining to **Online Behavioral Advertising** through a browser or **Device**—the **Participant** must apply that **Individual's** preference to the browser or **Device** from which the preference was exercised and any browser and **Device** associated through **Cross-Device Tracking** for compliance with this requirement**.**
Required	**TrustArc P&DG IMPLEMENT Standard:** *Choice and Consent:* Enable individuals to choose whether personal data about	**18. Clear and Conspicuous Access to Choice Mechanisms** Requirement: Privacy preference management tools must be intuitive, reliable, and easy for **Individuals** to use. They must list the **Participant** along with other parties that collect and use data for **Online Behavioral Advertising** purposes, and allow **Individuals** to opt-out of any or all of the listed parties.

	them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. 2018 NAI Code of Conduct II.C.2	Access to preference management tools shall be **Clear and Conspicuous** as outlined in these Assessment Criteria. In cases when additional steps are required by **Individuals** to exercise a preference, **Individuals** must be provided **Clear and Conspicuous** notice at each step on how to do this. Evaluation: TRUSTe must verify that the **Participant's** privacy preference management tools are intuitive, reliable, and easy for **Individuals** to use; list the **Participant** and other parties that collect and use data for **Online Behavioral Advertising** purposes; and allow **Individuals** the ability to opt-out of any or all of them. Gap and Remediation: If the **Participant's** privacy preference management tools are not intuitive, reliable, and easy for **Individuals** to use; do not list the **Participant** and other parties that collect and use data for **Online Behavioral Advertising** purposes; and/or do not allow **Individuals** the ability to opt-out of any or all of the listed parties, TRUSTe must inform the **Participant** that, for compliance with this requirement, its privacy preference management tools must: ● must be intuitive, reliable, and easy for **Individuals** to use; ● list the **Participant** and other parties that collect and use data for **Online Behavioral Advertising** purposes; and ● allow **Individuals** the ability to opt-out of any or all of the listed parties.
Required	**TrustArc P&DG IMPLEMENT Standard:** *Choice and Consent:* Enable individuals to choose whether personal data about them is processed.	**19. Communication of Preference in the Ad Chain** Requirement: The **Participant** must do the following to ensure the **Individual's** preference is both communicated to, and persistently honored by, the **Participant**: ● If technically capable (such as **SSPs, Ad Exchanges, Ad Mediators**), check or collect, and communicate these preferences to the other partners in the ad chain to ensure they can be persistently honored across all ad platforms (e.g. **DSPs**). ● **SSPs**, **Ad Mediators**, **DMPs**, and other **Participants** that do not otherwise collect **Individual** data must:

	Obtain and document prior permission where necessary and appropriate, and enable individual to opt-out of ongoing processing. 2018 NAI Code of Conduct II.C.5	○ read the **Individual's** privacy preference either stored in the browser, **Device**, or by an approved provider of privacy management solutions; ○ ensure every **Ad Transaction** has an associated privacy preference (if one exists) easily accessible by all entities within the ad ecosystem; and ○ communicate preferences to other entities within the ad chain (e.g., **DSPs**) in order to ensure that they can be persistently honored across all ad platforms (e.g., **DSPs**). ○ **Ad Networks, Ad Servers**, *and* **DSPs** must honor preferences received. Evaluation: TRUSTe must verify that the **Participant** does the following to ensure that **Individuals'** preferences are both communicated to, and persistently honored by, the **Participant**: ● if the **Participant** is technically capable (such as **SSPs, Ad Exchanges, Ad Mediators**), checks or collects, and communicates these preferences to the other partners in the ad chain to ensure they can be persistently honored across all ad platforms (e.g., **DSPs**). ● **SSPs**, **Ad Mediators**, **DMPs**, and other **Participants** that do not otherwise collect **Individual** data shall: ○ read the **Individual's** privacy preference either stored in the browser, **Device**, or by an approved provider of privacy management solutions; ○ ensure every **Ad Transaction** has an associated privacy preference (if one exists) easily accessible by all entities within the ad ecosystem; and ○ communicate preferences to other entities within the ad chain (e.g., **DSPs**) in order to ensure that they can be persistently honored across all ad platforms (e.g., **DSPs**). ○ **Ad Networks, Ad Servers**, *and* **DSPs** must honor preferences received. Gap and Remediation: If the **Participant** cannot verify that it does all of the following to ensure **Individuals'** preferences are communicated to, and persistently honored by, the

		Participant, TRUSTe must inform the **Participant** that it must ensure that **Individuals'** preferences are communicated to, and persistently honored by, the **Participant**, by: ● if the Participant is technically capable (such as SSPs, Ad Exchanges, Ad Mediators), checking or collecting, and communicating these preferences to the other partners in the ad chain to ensure they can be persistently honored across all ad platforms (e.g., DSPs). ● SSPs, Ad Mediators, DMPs*,* and other Participants that do not otherwise collect Individual data by: ○ reading the Individual's privacy preference either stored in the browser, Device, or by an approved provider of privacy management solutions; ○ ensuring every Ad Transaction has an associated privacy preference (if one exists) that is easily accessible by all entities within the ad ecosystem; and ○ communicating preferences to other entities within the ad chain (e.g., DSPs) in order to ensure that they can be persistently honored across all ad platforms (e.g., DSPs). ○ Ensuring Ad Networks, Ad Servers*, and* DSPs honor preferences received.
Conditional	**TrustArc P&DG IMPLEMENT 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	**20. Right to Withdraw Consent** Requirement: The **Participant** will provide **Individuals** with mechanisms to: ● withdraw previously given **Express Consent** or change their choice selection; and ● to easily opt-out of ongoing processing about them with respect to the collection and use of their data for **Online Behavioral Advertising**. Evaluation: TRUSTe must verify that the **Participant** provides **Individuals** with mechanisms to withdraw their previously given **Express Consent** or change their choice selection, and to easily opt-out of any ongoing collection or use of their **Personal Information** for **Online Behavioral Advertising**.

	opt-out of ongoing processing. DAA Self-Regulatory Principles for Online Behavioral Advertising III.B.2, European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the European Self Regulatory Programme on OBA 2.8.4	Gap and Remediation: If the **Participant** does not provide individuals with such mechanisms, TRUSTe must inform the **Participant** that, for compliance with this requirement, it must provide Individuals with mechanisms to: ● withdraw previously given **Express Consent** or change their choice selection; and ● to easily opt-out of ongoing processing about them with respect to the collection and use of their data for **Online Behavioral Advertising**.

Data Collection Certification Assessment Criteria

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. 3 Total Requirements 0 Required 3 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Conditional	**TrustArc P&DG IMPLEMENT 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. 2018 NAI Code of Conduct II.F.1	**21. Right of Access** Requirement: The **Participant** must provide **Individuals** with reasonable access to data collected about them, and other information associated with that data collection, that is retained for the purposes of **OBA** or other marketing purposes. If the **Participant** collects **Contact Information** or **Sensitive Information** directly from an **Individual**, about that **Individual**, the **Participant** must have available, operational, and understandable policies to enable the **Individual** to: ● access and correct his or her **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 **Contact Information** or **Sensitive Information** collected or gathered about that **Individual**, provided such request to **Contact Information** or **Sensitive 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 **Contact**

		Information or **Sensitive 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 **Contact Information** or **Sensitive Information**. The request must be responded to within a reasonable timeframe following an **Individual's** request for access (e.g., 45 days) and the **Contact Information** or **Sensitive Information** must be provided to **Individuals** in an easily comprehensible way. The **Participant** is not required to provide an **Individual** access **Contact Information** or **Sensitive Information** to the extent that: ● such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach **Participant's** confidential information or the confidential information of others; ● the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However, the **Participant** may not deny access on the basis of cost if the **Individual** offers to pay the costs of access; ● the requested **Contact Information** or **Sensitive Information** is derived from public records or is **Publicly Available Information** and is not combined with non-public record or non-publicly available information; or ● other laws or regulations prevent the provision of such access. 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 **Contact Information** or **Sensitive 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 fulfilled. 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 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.
Conditional	**TrustArc P&DG IMPLEMENT 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. GDPR Articles 17 and 19	**22. Right to Erasure** Requirement: Where appropriate and in accordance with applicable law, the **Participant** must enable **Individuals** to delete **Contact Information** or **Sensitive Information** that is **Processed** by the **Participant** or **Third Parties** acting on the **Participant's** behalf (e.g., **Processors**). The **Participant** must delete **Contact Information** or **Sensitive 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 **Contact Information** or **Sensitive Information** to any recipients of the **Contact Information** or **Sensitive Information** to whom **Contact Information** or **Sensitive Information** have been disclosed, including any third-party **Processors**.

		The **Participant's** processes or mechanisms for deletion of **Contact Information** or **Sensitive Information** by the **Individual** 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 **Contact Information** or **Sensitive Information**. The request must be responded to within a reasonable timeframe following an **Individual's** request for deletion (e.g., 1 month), and the **Contact Information** or **Sensitive 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 Contact Information** or **Sensitive 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**, **First Party,** or **Third Party** 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 **First Party** or **Third Party**; ● 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 that the **Participant** has procedures in place to respond to such requests. If the **Participant** identifies an applicable qualification to not delete **Individuals' Contact Information** or **Sensitive 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. Where the **Participant** identifies an applicable qualification, TRUSTe must verify whether the applicable qualification is justified.
Conditional	**TrustArc P&DG IMPLEMENT 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. Privacy Rights for California Minors in the Digital World Section 1 Chapter 22.1 22581(a)(1)	**23. Information Relating to Under Age 18 Individuals** Requirement: If **Participant** collects any **Personal Information** from an **Individual** under the age of 18, then **Participant** must implement a reasonable and appropriate mechanism to allow the **Individual** to have such **Personal Information** deleted or permanently de-identified. Evaluation: TRUSTe must verify that, if the **Participant** collects any **Personal Information** from an **Individual** under the age of 18, the **Participant** has a reasonable and appropriate mechanism in place to allow the **Individual** to have such **Personal Information** deleted or permanently de-identified. Gap and Remediation: If the **Participant** does not have a reasonable and appropriate mechanism in place to allow **Individuals** under the age of 18 to delete or permanently de-identify their **Personal Information**, TRUSTe must inform the **Participant** that a reasonable and appropriate mechanism must be in place for compliance with this requirement.

Data Collection Certification Assessment Criteria

DATA INTEGRITY AND QUALITY Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use. 1 Total Requirements 1 Required 0 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT Standard:** *Data Integrity and Quality:* Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use. GDPR Article 5(1)(d)	**24. Data Integrity and Quality** Requirement: The **Participant** must take steps to verify that the data 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 data 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 ensure that the data it maintains 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 reasonable procedures in place, TRUSTe must inform the **Participant** that procedures to verify and ensure that the data it maintains up to date, accurate, and complete, to the extent necessary for the purposes of use, are required for compliance with this requirement.

Data Collection Certification Assessment Criteria

SECURITY Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. 4 Total Requirements 3 Required 1 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG IMPLEMENT Standard:** *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. GDPR Article 32(1), GDPR Article 32(2) ISO 27001 8.1 Operational Planning and Control and 8.3 Information Security Risk Treatment 2018 NAI Code of Conduct II.F.3	**25. Security of Processing** Requirement: The **Participant** must implement reasonable physical, technical and administrative safeguards, including without limitation applicable policies, to protect data 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 data 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 **Processors** (e.g., agents, business associates, service providers, vendors) to which data is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure, or other misuses of the data.

Data Collection Certification Assessment Criteria

	DAA Self-Regulatory Principles for Online Behavioral Advertising IV.A DAA Application of Self-Regulatory Principles to the Mobile Environment IX European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.1.1	These safeguards may include: ● 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, including without limitation applicable policies, 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, including without limitation applicable policies, or inadequate safeguards to protect **Personal Information**, TRUSTe must inform the **Participant** that the implementation of such safeguards, including without limitation applicable policies, are required for compliance with this requirement.
Conditional	**TrustArc P&DG IMPLEMENT Standard:** *Security:* Protect data from loss, misuse, and	**26. Technology Controls**

	unauthorized access, disclosure, alteration, or destruction. 2018 NAI Code of Conduct II.F.3 DAA Self-Regulatory Principles for Online Behavioral Advertising IV.A DAA Application of Self-Regulatory Principles to the Mobile Environment IX European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.1.1	Requirement: The **Participant**, depending on its role in the ad ecosystem, must use a unique domain name for all technologies (e.g., cookies, device recognition technology, and scripts) to separate any individual technology used for **Online Behavioral Advertising** purposes from one that is not used for **Online Behavioral Advertising** purposes (e.g., analytics). For cookie-based preference management systems, the **Participant** shall use the same cookie name for all of its opt-out mechanisms. For example, the opt-out cookie set for the DAA opt-out mechanism has the same name as the cookie set for the NAI opt-out mechanism. Cookie-based preference management systems, web-based technologies or other mechanisms used to manage opt-out preferences must have a persistency of five years to adequately honor **Individuals'** preferences. Mobile-based technologies or other mechanisms used to manage opt-out preferences must have a persistency of 24 months to adequately honor **Individuals'** preferences. Evaluation: TRUSTe must verify that the **Participant** uses a unique domain name to separate any individual technology used for **Online Behavioral Advertising** purposes from one that is not used for **Online Behavioral Advertising** purposes. Gap and Remediation: If the **Participant** does not use a unique domain name for all technologies to separate any individual technology used for **Online Behavioral Advertising** purposes from one that is not used for **Online Behavioral Advertising** purposes, TRUSTe must inform the **Participant** that unique domain names for technologies used for **Online Behavioral Advertising** purposes are required for compliance with this requirement.

Data Collection Certification Assessment Criteria

Required	**TrustArc P&DG IMPLEMENT Standard:** *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. GDPR Articles 33-34 ISO 27001 8.1 Operational Planning and Control	**27. 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**. Gaps and Remediation: If the **Participant** does not have these procedures and mechanisms in place, TRUSTe must inform the **Participant** that incident detection, escalation, and management procedures and mechanisms to determine whether an incident involves **Personal Information** must are required for compliance with this requirement.
Required	**TrustArc P&DG IMPLEMENT Standard:** *Security:* Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.	**28. 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 that the **Participant** has policies and procedures in place for conducting these assessments, and remediating areas of identified risk.

Data Collection Certification Assessment Criteria

	GDPR Article 32(2) ISO 27001 8.2 Information Security Risk assessment and 8.3 Information Security Risk Treatment	Gaps and Remediation: If the **Participant** does not have policies and procedures in place for conducting these assessments and for 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. 4 Total Requirements 2 Required 2 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Conditional	**TrustArc P&DG IMPLEMENT Standard**: *Transparency*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. 2018 NAI Code of Conduct II.B.6	**29. Enhanced Notice** Requirement: The **Participant,** depending on its role in the ad ecosystem must provide **Individuals** with an enhanced notice in clear and plain language that informs **Individuals** of the following: • what data is collected, either through active or passive means, and how the data is used with respect to **Online Behavioral Advertising**; • the means by which **Individuals** can express their privacy preference with respect to **Online Behavioral Advertising** and instructions; • description of the effects of exercising a privacy preference; and • how an **Individual's Device** was identified if using **Device Recognition Technology**.

Data Collection Certification Assessment Criteria

	DAA Self-Regulatory Principles for Online Behavioral Advertising II.A.2 DAA Application of Self-Regulatory Principles to the Mobile Environment III.A.2 Application of the DAA Principles of Transparency and Control to Data Used Across Devices Control FN3	Evaluation: TRUSTe must verify that the **Participant** provides the **Individual** with an enhanced notice in clear and plain language that informs **Individuals** of the required information. Gaps and Remediation: If the **Participant** does not provide this required information in an enhanced notice, TRUSTe must inform the **Participant** that the required information must be provided in an enhanced notice for compliance with this requirement.
Conditional	**TrustArc P&DG IMPLEMENT Standard**: *Transparency*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. 2018 NAI Code of Conduct II.B.6 DAA Self-Regulatory Principles for Online	**30. Provision of Enhanced Notice** Requirement: The **Participant**, depending on its role in the ad ecosystem, must provide **Clear and Conspicuous** enhanced notice regarding its **Online Behavioral Advertising** data collection, use, and choice practices**,** including notice of third parties with whom such data may be shared. To provide this enhanced notice, the **Participant** must make available access to easy-to-find-and-use preference management tools that include a universal choice mechanism. **Ad Networks**, **Ad Servers**, and **DSPs** must provide enhanced notice and access to preference management tools through an in-ad notice via an **Icon**, “Ad Preferences”, or similarly labeled button, or direct link.

	Behavioral Advertising II.A.2 DAA Application of Self-Regulatory Principles to the Mobile Environment IV.A.3	Enhanced notice may be provided through the app or web page where data is collected if there is an arrangement with the **First Party**. If more than one **Ad Company** is involved in the ad chain, the **Participant**, if the **Participant** is not directly serving the ad to the **Individual**, will verify that the **Ad Company** directly involved provides enhanced notice and access to preference management tools. Enhanced notice is not required if data is only collected or received for the following purposes: ● operations and systems management including: ○ intellectual property protection; ○ compliance, public purpose, and consumer safety; ○ authentication, verification, fraud prevention, and security; ○ billing or product or service fulfillment; or ○ Ad Reporting or Ad Delivery; and ● market research or product development including the analysis of the characteristics of a group of consumers or market, and product performance to improve existing or new products using de-identified data that has been de-identified in such a way that an Individual cannot be re-identified. Evaluation: TRUSTe must verify the **Participant** provides **Clear and Conspicuous** enhanced notice regarding its **Online Behavioral Advertising** data collection, use, and choice practices **,** including notice of third parties with whom such data may be shared; and that the **Participant** has easy-to-find-and-use preference management tools in place that include a universal choice mechanism. Gaps and Remediation: If **Clear and Conspicuous** enhanced notice is not provided, or if an easy-to-find-and-use preference management tool is not in place,

Data Collection Certification Assessment Criteria

		TRUSTe must inform the **Participant** that providing **Clear and Conspicuous** enhanced notice regarding its **Online Behavioral Advertising** data collection, use, and choice practice**,** including notice of third parties with whom such data may be shared.s; and providing easy-to-find-and-use preference management tools that include a universal choice mechanism are required for compliance with this requirement.
Required	**TrustArc P&DG IMPLEMENT Standard**: *Transparency*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. 2018 NAI Code of Conduct II.B.1 DAA Self-Regulatory Principles for Online Behavioral Advertising II.A. DAA Application of Self-Regulatory Principles to the Mobile Environment IV.A.2	**31. Comprehensive Privacy Notice** Requirement: In clear and plain language, the **Participant's Privacy Notice** must inform **Individuals** of the following: ● the scope of the **Privacy Notice** including data collected for **Online Behavioral Advertising** or non-online behavioral advertising purposes; ● what types of data, including **Personal Information**, **Device-Identifiable Information**, **Precise Geo-location Data**, and **Personal Directory Data** are collected, either through active or passive means; ● the type of entity(ies) including **Processor**s, that assist the **Participant** in collection and use of the data; ● how the collected data will be used, including whether the data is used for **Online Behavioral Advertising** or non-online behavioral advertising purposes; ● whether collected data is tied to or otherwise linked to **Personal Information**; ● whether the collected data is shared with **Third Parties**, including **Processors**, the types of **Third Parties** the data is shared with, and whether those **Third Parties** use the data for targeted advertising purposes; ● names or a link to a list of the names of the **Third Parties** not acting as **Processors** with whom **Contact Information** or **Sensitive Information** is shared;

Data Collection Certification Assessment Criteria

	Application of the DAA Principles of Transparency and Control to Data Used Across Devices Transparency European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.5	• general description of the techniques and technologies the **Participan**t uses to collect data about **Individuals'** online or offline behavior, or app or web usage activity including but not limited to the use of cookies, pixels, **Device Recognition** techniques, or LSO's; • whether the **Participant** supplements the data it collects with data from **Third Part**y sources, the types of data it receives, and types of **Third Party** sources it receives data from; • how **Individuals** can exercise their preferences, including the ability to withdraw consent, regarding the collection or use of data for **Online Behavioral Advertising** purposes, including for third parties with whom such data may be shared, and obtain access to privacy preference management tool.; • how **Individuals** can exercise their data protection rights and request access to **Contact Information** or **Sensitive Information** for the purpose of correcting inaccuracies, updating it, or to request deletion; • how long collected data is retained; • generally, the types of security measures in place to protect collected data; • as applicable, a statement of the **Participant's** compliance with self-regulatory frameworks such as the DAA or NAI; • that collected data 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; • how the **Individual** will be notified of any **Material Changes** in the **Participant's Online Behavioral Advertising** data collection or use policies, and practices; • how the **Individual** can contact the **Participant**, including company name, email address or a link to an online form, and physical address; • the effective Date of Privacy Notice; and • the independent dispute resolution body designated to address complaints.

Data Collection Certification Assessment Criteria

		Evaluation: TRUSTe must verify the **Participant** provides **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.
Required	**TrustArc P&DG IMPLEMENT Standard**: *Transparency*: Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights. 2018 NAI Code of Conduct II.B.1 DAA Self-Regulatory Principles for Online Behavioral Advertising II.A.1 European Interactive Digital Advertising Alliance Self-certification Criteria for companies participating in the	**32. Provision of Privacy Notice** Requirement: The **Participant** must provide a **Clear and Conspicuous Privacy Notice** on its online properties, including its web site, regarding its privacy practices around **Online Behavioral Advertising**, or multi-site or **Cross-App Data** collection. Access to the **Privacy Notice** shall be **Clear and Conspicuous**, and at a minimum be accessible from the homepage of the **Participant**'s Web site. The **Participant** must provide copies of all applicable **Privacy Notices** and/or hyperlinks to the same. Evaluation: TRUSTe must verify the **Participant** provides a **Clear and Conspicuous Privacy Notice** regarding its privacy practices around **Online Behavioral Advertising** or **Cross-App Data** collection on its online properties. Gaps and Remediation: If a **Clear and Conspicuous Privacy Notice** is not provided, TRUSTe must inform the **Participant** that providing a **Clear and Conspicuous Privacy Notice** regarding its privacy practices around **Online Behavioral Advertising** or **Cross-App Data** collection on its online properties is required for compliance with this requirement.

Data Collection Certification Assessment Criteria

	European Self Regulatory Programme on OBA 2.6	

REPORTING AND CERTIFICATION Demonstrate the effectiveness of your program and controls to management, the Board of Directors, employees, customers, regulators, and the public. 1 Total Requirements 1 Required 0 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG DEMONSTRATE Standard**: *Reporting and Certification:* Demonstrate the effectiveness of your program and controls to management, the Board of Directors, employees, customers, regulators, and the public. DAA Self-Regulatory Principles for Online Behavioral Advertising I.	**33. Consumer Education** Requirement: The **Participant** must provide **Individuals** with access to educational information provided by industry self-regulatory organizations about **Online Behavioral Advertising.** Educational information must be accessible through preference management tools and through the **Participant's** website. Educational information must include at least the following information: ● a description of what **Online Behavioral Advertising** is; ● how the **Participant** collects, uses, and stores **Online Behavioral Advertising** data; and ● how the **Individual** can exercise their preference.

Data Collection Certification Assessment Criteria

	2018 NAI Code of Conduct II.A.2 European Interactive Digital Advertising Alliance Self-certification Criteriafor companies participating in the European Self Regulatory Programme on OBA 2.3	Evaluation: TRUSTe must verify that the **Participant** is providing the required educational information. Gaps and Remediation: If this information is not provided by the **Participant**, TRUSTe must inform the **Participant** that providing educational information is required for compliance with this requirement.

Data Collection Certification Assessment Criteria

RESOURCE ALLOCATION Establish budgets. Define roles and responsibilities. Assign personnel. 1 Total Requirements 1 Required 0 Conditional		
Type	**TrustArc P&DG Framework and External Regulatory Standard Mapping**	**Assessment Criteria**
Required	**TrustArc P&DG BUILD Standard**: *Resource Allocation:* Establish budgets. Define roles and responsibilities. Assign personnel. 2018 NAI Code of Conduct III.A.2.	**34. Appoint a Privacy Leader** Requirement: The **Participant** must designate one individual with the responsibility for managing the **Participant's** compliance with these Assessment Criteria and providing training to relevant staff within the **Participant's** organization. Evaluation: TRUSTe must verify that the **Participant** has designated one individual with the responsibility for managing the **Participant's** compliance with these Assessment Criteria and providing training to relevant staff within the **Participant's** organization. Gaps and Remediation: If the **Participant** has not designated one individual with the responsibility for managing the **Participant's** compliance with these Assessment Criteria and for providing training to relevant staff within the **Participant's** organization, TRUSTe must inform the **Participant** that an individual with these responsibilities must be designated..

Data Collection Certification Assessment Criteria

PROCESSES
Establish, manage, measure, and continually improve processes for establishing, implementing, publicizing, and actively managing a privacy complaint-handling process, including alternative dispute resolution as needed.

1 Total Requirements 1 Required 0 Conditional

Type	TrustArc P&DG Framework and External Regulatory Standard Mapping	Assessment Criteria
Required	**TrustArc P&DG BULD Standard**: *Processes:* Establish, manage, measure, and continually improve processes for PIAs, vendor assessments, incident management and breach notification, complaint handling, and individual rights management. 2018 NAI Code of Conduct III.C.2	**35. Privacy Complaint Mechanism** Requirement: The **Participant** must provide **Individuals** with reasonable, appropriate, simple, and effective mechanisms to submit complaints, express concerns, and provide feedback regarding the **Participant's** privacy practices at no cost to **Individuals**. Evaluation: TRUSTe must verify that the **Participant** has mechanisms in place for **Individuals** to submit submit complaints, express concerns, and provide feedback regarding the **Participant's** privacy practices at no cost to **Individuals**. Gaps and Remediation: If the **Participant** does not have mechanisms in place for **Individuals** to submit complaints, express concerns, and provide feedback regarding the **Participant's** privacy practices at no cost to **Individuals**, TRUSTe must inform the **Participant** that such mechanisms are required for compliance with this requirement.

Data Collection Certification Assessment Criteria

III. DEFINITIONS

A. "Ad Company" is an entity that helps optimize or serve an ad, and includes the following types of entities. Note: a single entity may fall under multiple types.

1. "Ad Exchanges" are technology platforms that facilitate automated, auction-based pricing and buying of online advertising inventory in real-time. **Ad Exchanges** represent a sales channel to **App Developers**, website **Publishers**, and **Ad Networks**, and a source of online advertising inventory for advertisers and agencies.

2. "Ad Mediator" is an ad-tracking platform that is integrated with multiple Ad Networks at an API level, facilitating **Ad Networks'** management and ad optimization.

3. "Ad Network" is an entity that connects advertisers with **App Developers** and website **Publishers** that host online advertisements.

4. "Ad Server" is a computer system that stores, maintains and serves (uploads) advertising banners for one or more websites. Ad servers program, track, and report several statistics about website visitors which are used by advertisers to custom tailor ads and offers to suit different categories of visitors.

5. "Data Management Provider" ("DMP") is an entity that organizes and interprets unique demographic and interest-based information that allow **App Developers**, website **Publishers**, and advertisers to discover and target relevant audiences at scale.

6. "Demand Side Platform" ("DSP") is a system that allows advertisers to manage their bids across multiple **Ad Exchanges** in order to minimize expenses while maximizing results.

7. “Internet Service Provider (“ISP”)” is an entity that provides services for accessing, using, and participating on the internet.
8. “Real-time Bidding (RTB) Exchange” allows for the buying digital inventory from multiple **App Developers** and website **Publishers** on an impression-by-impression basis, typically involving an auction pricing mechanism.

9. “Supply Side Platform” (“SSP”) is a system that allows **App Developers** and website **Publishers** to automate the management of their inventory across multiple **Ad Exchanges** or **Ad Networks** for purposes of efficiency.

10. “Web browser provider” is an entity that develops and offers a software application for accessing information on the World Wide Web.

B. “Ad Delivery” means the delivery of online advertisements or advertising-related services using **Ad Reporting** data. **Ad Delivery** does not include the collection and use of **Ad Reporting** data when such data is used to deliver advertisements to a computer or **Device** based on the preferences or interests inferred from information collected over time and across non-**Affiliate** sites, because this type of collection and use is covered by the definition of **Online Behavioral Advertising**.

C. “Ad Reporting” means the logging of page views on a Web site(s) or the collection or use of other information about a browser, operating system, domain name, date and time of the viewing of the web page or advertisement, and related information for purposes including but not limited to:

1. Statistical reporting in connection with the activity on a website(s);

2. Web analytics and analysis; and

3. Logging the number and type of advertisements served on a particular website(s).

Data Collection Certification Assessment Criteria

D. “Ad Transaction” is the recorded exchange, movement or conveyance of ad related data, including money, between at least two parties.

E. “Affiliate” means an entity that controls, is controlled by, or is under common **Control** with, another entity.

F. “App Developer” is the entity that owns, **Controls**, and operates the mobile application with which the **Individual** interacts.

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

H. “Control” of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the **Control** of another entity and thus be treated as a **First Party** under these Assessment Criteria, the entity must adhere to the **Online Behavioral Advertising** policies that are not materially inconsistent with the other entity’s policies.

I. “Cross-App Data” is data collected from a particular device regarding applications use over time and across non-**Affiliated** applications.

J. “Cross-Device Tracking” is when an **Ad Company** or other entity tries to connect an **Individual’s** activity and behavior across multiple browsers and **Devices**.

K. “De-identification” is the process of removing the association between a set(s) of data and a specific **Individua**l, browser, or device.

Data Collection Certification Assessment Criteria

L. “Derived Product(s)” is a new product derived from an existing product which has different properties from the product it was derived from. For example, characterizations developed about a location based on longitude and latitude data is a derived product.

M. “Deterministic” is an algorithm, model, procedure, process, etc., whose resulting behavior is entirely determined by its initial state and inputs, and is not random or stochastic.

N. “Device” is a thing made or adapted for a particular purpose, typically a piece of electronic equipment that allows the user to process, receive, and send data.

O. “Device-Identifiable Information” is any data, such as **Persistent Device Identifiers**, that is linked to a specific device or browser but is not used, or intended to be used to identify a particular **Individual**. It includes **Cross-App Data**, if that data is not used or intended to be used to identify a particular **Individual**. It does not include data that has been subject to **De-Identification**.

P. “Device Recognition Technology” is either **Deterministic** or **Probabilistic** statistical identification approach based on the collection of information about the attributes of a discrete **Device** and browser combination used to identify and recognize the same **Device** at a later point in time.

Q. “Express Consent” means the affirmative consent to a practice by the **Individual** after being provided notice, but prior to implementing the practice.

R. “First Party” means the entity that is the owner of the website or app or has **Control** over the website or app with which the **Individual** interacts and its **Affiliates**.

S. “Icon” is an icon in or around an **Online Behavioral Advertisement** that that contains a link to the notice and preference management tool enabling **Individuals** to exercise choice.

Data Collection Certification Assessment Criteria

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

U. “Material Change” means degradation in the rights or obligations regarding the collection, use, or disclosure of data for an Individual. This usually includes any changes to Participant's:

1. Practices regarding notice, collection, use, and disclosure of data;

2. Practices regarding user choice and consent to how **Personal Information** is used and shared; or

3. Measures for information security, integrity, access, or **Individual** redress.

V. "Online Behavioral Advertising (OBA)" means the collection of data from a particular computer or device regarding Cross-App data or web viewing behaviors over time and across non-Affiliate apps or websites for the purpose of using such data to predict **Individual** preferences or interests to deliver advertising to that computer or **Device** based on the preferences or interests inferred from such web viewing behaviors. **Online Behavioral Advertising** does not include the activities of **First Parties**, **Ad Delivery** or **Ad Reporting**, or contextual advertising (i.e., advertising based on the content of the app or web page being visited, a **Individual’s** current visit to an app or web page, or a search query).

W. “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.

X. “Personal Directory Data” is data created by the **Individual** and stored on, and accessed through, a particular **Device**. Examples of **Personal Directory Data** include calendar, address book, phone/text log, and photo/video data.

Y. “Personal Information (PI)” is any information or combination of data about an identified or identifiable **Individual** that can be used to identify, contact, or locate that **Individual**. **PI** includes the following subcategories:

Data Collection Certification Assessment Criteria

1. “Contact Information” is information that can be used on its own to directly reach an **Individua**l. Examples of **Contact Information** include first and last name plus mailing or home address, email address, telephone or mobile phone numbers.

2. “Persistent Device Identifiers” are distinctive device characteristics, or numbers or alphanumeric characters that are associated with and used to recognize a specific app, browser cookie, or **Device**. Examples of **Persistent Device Identifiers** include IDFA, Android ID, IMEI, and MAC address.

3. “Precise Geo-location Data” is data that describes the precise real-time location of an **Individual** or a **Device**, and is derived using technologies such as GPS level longitude and latitude, or WiFi triangulation.

4. “Sensitive Information” is information where unauthorized use or disclosure of that information would be likely to cause financial, physical, or reputational harm to an **Individual**. Examples of **Sensitive Information** include:

    i. Financial Information such as credit card or bank account number;

    ii. Government-issued identifiers such as SSN, driver’s license number

    iii. Insurance plan numbers

    iv. Racial or ethnic origin of the Individual;

    v. Political opinions of the Individual;

    vi. Religious or similar beliefs of the Individual;

    vii. **Individual’s** trade union membership;

viii. Precise information regarding the **Individual's** past, present, or future physical or mental health condition and treatments including genetic, genomic, and family medical history;

ix. **Individual's** sexual life or orientation;

x. History of **Precise Geo-location Data** associated with a single device;

xi. The commission or alleged commission of any offense by the **Individual**; or

xii. Any proceedings for any committed or allegedly committed offense by the Individual and the disposal or such proceedings or the sentence of any court in such proceedings.

Z. "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.

AA. "Probabilistic" is the situation or model where there are multiple possible outcomes, each having varying degrees of certainty or uncertainty of its occurrence.

BB. "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, Processors acting as an agent or vendor, or vendors.

CC. "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.

Data Collection Certification Assessment Criteria

DD. "Publicly Available Information [PAI]" means any information reasonably believed to be lawfully made available to the general public from:

1. Federal, state or local government records;

2. Widely available source(s) having no additional prohibition around onward transfer or use; or

3. Disclosures to the general public that are required to be made by federal, state or local law.

EE. "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**.

FF. "Website Publisher" is the entity that owns, Controls, and operates the website (including Mobile websites) with which the **Individual** interacts.