ANNEX C

TRUSTe has developed a set of privacy standards[1] used to certify companies under its Privacy Certification program and has used these requirements as a basis for demonstrating that Accountability Agent Recognition Criteria 4 has been met.[2] *TRUSTe will offer CBPR certification as a unique seal. TRUSTe will post the program requirements associated with this unique seal separately from the Website Privacy Program Requirements as modification of certain existing requirements was necessary in order to successfully map against the CBPR program requirements (see discussion herein). TRUSTe will expressly incorporate all language stipulated in Column III (Relevant Program Requirement* **)** *into the unique CBPR Program Requirements. In addition TRUSTe will publically post this signed Recommendation Report.*

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS MAP

NOTICE 2

COLLECTION LIMITATION 8

USES OF PERSONAL INFORMNATION 10

CHOICE 18

INTEGRITY OF PERSONAL INFORMATION 25

SECURITY SAFEGUARDS 30

ACCESS AND CORRECTION 39

ACCOUNTABILITY 44

[1] These privacy standards are available at http://www.truste.com/privacy-program-requirements/program_requirements_website_privacy

[2] Note that TRUSTe's *Master Services Agreement* (referenced in questions 7 and 40) is business confidential. Pursuant to the terms of the JOP Charter, this information is not included in this report, since this report is to be made publicly available. Should an Economy have further questions on this documentation, please contact the JOP.

NOTICE

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement (Provided by TRUSTe)**
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is	(III.D.2-6) • At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant's information practices. • Access to the Privacy Statement shall be Clear and Conspicuous. • As reasonable, Privacy statement must be available when the Individual engages with the Participant, such as through an application, Website homepage or landing page. • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. • TRUSTe does not distinguish between online and offline collected data in its program requirements, and therefore covers both. (III.D.1) • Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe in its sole discretion that states Participant's information practices and is in conformance with these Program Requirements (III.D.1.a) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. (III.D.1.k) • Effective date of Privacy Statement

	justified.	
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	(III.D.2-6) • At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant's information practices. (III.D.1.a) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. (III.D.1.c) • Whether PII is appended with information obtained from third party sources.
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(III.D.1.a) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. (III.C.1.a (1-2) • Participant shall only collect PII where such collection is: o Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or o With notice to and consent of the Individual

1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(III.D.1.a) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. (III.D.1.b) • What types of Third Parties if any, including Service Providers, collected information is shared with.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(III.D.1.h) • How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address.
1.e) Does this privacy	Where the Applicant answers **YES**, the	(III.D.1.a)

statement provide information regarding the use and disclosure of an individual's personal information?	Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	• What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. (III.D.1.b) • What types of Third Parties if any, including Service Providers, collected information is shared with.
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability	(III. C.5.a-f) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant • Such mechanism or process shall be clear, conspicuous, and easy to use • Such mechanism or process shall confirm to the Individual inaccuracies have been corrected. • Participant's privacy statement shall state how access is provided

	Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.C.2.a) • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. [NOTE: *TRUSTe stipulates that the above notice requirements around use cover both first and third parties and do not distinguish between first and third parties*.]

	qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	(III.C.2.a) • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. (III.D.1.b) • What types of Third Parties if any, including Service Providers, collected information is shared with.

COLLECTION LIMITATION

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement (Provided by TRUSTe)**
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	(III.D.1.a,c) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used; • Whether PII is appended with information obtained from third party sources.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use	• What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used.(III.D.1.a) (III.C.1.a.1-2) • Participant shall only collect PII where such collection is: • Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or • With notice to and consent of the Individual (III.C.2.a-b)

	with the stated purpose of collection. Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	• Use of PII • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. • Information collected by the Participant or the Participant's Service Provider may be used to tailor the Individual's experience on the Participant's Online property.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	(*Master Services Agreement* section 6(b)(ii) and 6(b)(iii)) Participant will not display any of the TRUSTe Mark(s) on any Web site that is, or offers any service or product that is, misleading, unlawful, or violative of the rights of third parties. Participant represents that it understands that its participation in, and compliance with, any Program does not constitute specific compliance with any law or regulation. Participant represents that it understands that it has an independent duty to comply with any and all laws and regulations. *[NOTE: For purposes of CBPR certification, TRUSTe agrees to incorporate language in its Master Services Agreement that requires "that all collection by a CBPR certified organization must be collected by fair means without deception".*

USES OF PERSONAL INFORMATION

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria** **(*to be verified by the Accountability Agent*)**	**Relevant Program Requirement (Provided by TRUSTe)**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	(III. C. 2.a) • Use of information is limited to "the provision of those services advertised or provided for and in accordance with their posted privacy statement in effect at the time of collection or with notice and consent as described in these program requirements." Thus use is limited to the purpose stated within the privacy statement.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the	(III.D.6.m) • Participant shall treat all collected information in accordance with the posted Privacy Statement in effect at the time of collection unless the Individual otherwise has given Express Consent. (III.C.3c) • Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process. (III.C.3c) • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or

9.b) Compelled by applicable laws?	personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify). Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.

10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or	(III.C.1) • Participant shall only collect PII where such collection is: • Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or • With notice to and consent of the Individual (III.C.2) • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. (III.D.1.a-b) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. • What types of Third Parties if any, including Service Providers, collected information is shared with. (III.C.3.b-c) • Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process. • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.

	related purposes.	
11. Do you transfer personal information to personal information processors? If YES, describe.		(III.C.1) • Participant shall only collect PII where such collection is: • Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or • With notice to and consent of the Individual • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. (III.C.2) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. • What types of Third Parties if any, including Service Providers, collected information is shared with. (III.D.1.a-b) • Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process. (III.C.3.b-c) • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or

		disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		(III.C.1) • Participant shall only collect PII where such collection is: • Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or • With notice to and consent of the Individual (III.C.2) • Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements. (III.D.1.a-b) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used. • What types of Third Parties if any, including Service Providers, collected information is shared with. (III.C.3.b-c) • Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process. • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or

		disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal	(III.C.3.b-e) • Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process. • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual. • Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control • Such mechanism shall be easy to use and offered at no cost to the Individual (III.C.3.a.1-2) • Participant shall offer the Individual control over their collected Personally Identifiable Information as follows: • Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose. • Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected.

	information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

CHOICE

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.D.1.d) • How and when the Individual can exercise choice as required in these Program Requirements. (III.C.3.a.1-2) • Participant shall offer the Individual control over their collected Personally Identifiable Information as follows: • Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose. • Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected.

	Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.D.1.d) • How and when the Individual can exercise choice as required in these Program Requirements. (III.C.3.a.1-2) • Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose. • Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected. (III.C.3.c) • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.

	or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
b16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.D.1.b) • What types of Third Parties if any, including Service Providers, collected information is shared with. (III.D.1.d) • How and when the Individual can exercise choice as required in these Program Requirements. (III.C.3.a.1-2)

	• Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the	• Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose. • Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected. (III.C.3.c) • Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.

	disclosure of their personal information must be provided.	
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.D.3) • Access to the Privacy Statement shall be Clear and Conspicuous. (III.D.1.a,c, d) • What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used • What types of Third Parties if any, including Service Providers, collected information is shared with; • How and when the Individual can exercise choice as required in these Program Requirements.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	(III.D.5) • Privacy statement must be available at the point where the Individual provides PII, or through a common footer. (III.D.3) • Access to the Privacy Statement shall be Clear and Conspicuous. (III.C.3.d-e) • Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control • Such mechanism shall be easy to use and offered at no cost to the Individual
19. When choices are	Where the Applicant answers **YES**, the	(III.C.3.d-e)

provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	• Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control • Such mechanism shall be easy to use and offered at no cost to the Individual
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that	(III.C.3.a.3-4) • Participant shall offer the Individual control over their collected Personally Identifiable Information as follows: o Participant shall honor and maintain the Individual's choice selection in a persistent manner until such time the Individual changes that choice selection; and o Participant shall provide a means by which the Individual may change their choice selection. (III.C.3.d-e) • Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control • Such mechanism shall be easy to use and offered at no cost to the Individual

	choices, when offered, can be honored, must be provided.	

INTEGRITY OF PERSONAL INFORMATION

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement (Provided by TRUSTe)**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	(III.E.3.a-b) • Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used. • If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information, as appropriate, based on the results of the investigation.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from	(III.E.3.a-b) • Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used. • If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information, as

Provide a description in the space below or in an attachment if necessary.	individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	appropriate, based on the results of the investigation. (III.C.5.a-f) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used. • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant • Such mechanism or process shall be clear, conspicuous, and easy to use • Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and • Participant's privacy statement shall state how access is provided.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the	(III.E.3.a-b) • Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used. • If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information, as appropriate, based on the results of the investigation. (III.C.5.a-f) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used. • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant

information was transferred? If YES, describe.	Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	• Such mechanism or process shall be clear, conspicuous, and easy to use • Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and • Participant's privacy statement shall state how access is provided. (III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: • Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or • Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and • Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII. [NOTE: *TRUSTe stipulates that the obligation of the participant under III.E.3.a-b also obligates the service provider pursuant to section III.E.5.a.1 – 2.*]
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be Appropriate to the size of the Participant's business; and • Appropriate to the level of sensitivity of the data collected and stored (III.E.3.a) • Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such

whom the personal information was disclosed? If YES, describe.		information is to be used. (III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: • Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or • Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and • Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII. [NOTE: *TRUSTe stipulates that III.E.3a requires steps by the participant to ensure data received from third parties is accurate and requires any third party to report incorrect data to the participant such that the participant is then able to conform to the requirements in this section*.]
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or	(III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: • Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or • Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and • Abide by the rights and obligations attached to the PII by the

of-date?	outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII. (III.E.3.a) • Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.

SECURITY SAFEGUARDS

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement (Provided by TRUSTe)**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	(III.E.2a) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be • Appropriate to the size of the Participant's business; and • Appropriate to the level of sensitivity of the data collected and stored (III.E.2a-e) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution. • Participant shall maintain and audit internal information technology systems within Participant's control such as: o Regularly monitor and repair systems including servers and desktops for known vulnerabilities; o Limit access and use of PII, or Third Party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or

	safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	Third Party PII, could cause financial, physical, or reputational harm to the Individual; o Implement protection against phishing, spam, viruses, data loss, and malware; and o Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual • Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual. • Access to PII or Third Party PII retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual. • Privacy Statement shall state that security measures are in place to protect collected PII and/or Third Party PII.
28. Describe how the safeguards you identified in response to question	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E.

27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	• Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2c) • Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2a-b.1-4) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution. • Participant shall maintain and audit internal information technology systems within Participant's control such as: o Regularly monitor and repair systems including servers and desktops for known vulnerabilities; o Limit access and use of PII, or Third Party PII, to personnel with a legitimate

	Applicant that the existence of such procedures are required for compliance with this principle.	business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the Individual; o Implement protection against phishing, spam, viruses, data loss, and malware; and o Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual [NOTE: *TRUSTe stipulates that "reasonable security measures" under III.E.2a include a requirement of staff engagement and training on the importance of maintaining the security of personal information*.]
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2a-e) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution. • Participant shall maintain and audit internal information technology systems within Participant's control such as: o Regularly monitor and repair systems including servers and desktops for known vulnerabilities; o Limit access and use of PII, or Third Party PII, to personnel with a legitimate

and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?		business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the Individual; o Implement protection against phishing, spam, viruses, data loss, and malware; and o Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual • Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual. • Access to PII or Third Party PII retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual. • Privacy Statement shall state that security measures are in place to protect collected PII and/or Third Party PII. [NOTE: *TRUSTe stipulates that a determination of the sensitivity of the information under III.E.1a(1) incorporates consideration of the severity of the harm.*]
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	(III.E.4) • If a Participant receives and retains PII or Third Party PII, the Participant must limit its retention to no longer than useful to carry out its business purpose, or legally required; and must disclose in their Privacy Statement how long they will retain that information. • Regardless of the time period of retention, so long as a Participant has PII or Third Party PII in its possession or control, the requirements included herein

		shall apply to such information.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2a-b (1-4) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution. • Participant shall maintain and audit internal information technology systems within Participant's control such as: o Regularly monitor and repair systems including servers and desktops for known vulnerabilities; o Limit access and use of PII, or Third Party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the Individual; o Implement protection against phishing, spam, viruses, data loss, and malware; and o Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2a-b (1-3) • Participant must implement reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution. • Participant shall maintain and audit internal information technology systems within Participant's control such as: o Regularly monitor and repair systems including servers and desktops for known vulnerabilities; o Limit access and use of PII, or Third Party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the Individual; o Implement protection against phishing, spam, viruses, data loss, and malware; and
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be

	privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.2.b) • Participant shall maintain and audit internal information technology systems within Participant's control such as: Regularly monitor and repair systems including servers and desktops for known vulnerabilities;
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this section III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII. [NOTE*: TRUSTe stipulates that III.E.5.a requires the participant to impose*

promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		*equivalent obligations on its third party service providers. As such, third-party service providers must provide notice to the participant for any data breach, including leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information.*]

ACCESS AND CORRECTION

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** **(Provided by TRUSTe)**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where	(III.C.5.a-h) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used. • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant • Such mechanism or process shall be clear, conspicuous, and easy to use • Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and • Participant's privacy statement shall state how access is provided. (IV.A.1.a-b) • Participant must provide an Individual with access to PII within thirty (30) calendar days of request. • If Participant does not provide an Individual the requested access within thirty (30) calendar days of the Individual's request, Participant must provide the Individual with a timeline establishing when the requested access will be provided. • Privacy Statement shall disclose the timeline establishing when the Individual can expect a response to their request for access.

	the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be	(III.C.5.a-h) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used. • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant • Such mechanism or process shall be clear, conspicuous, and easy to use • Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and • Participant's privacy statement shall state how access is provided. • Participant is not required to permit Individual access to Personally Identifiable Information to the extent that: o Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others; o The burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However,

37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.	required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or o The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information. • If Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access. (IV.A.1.a-b) • Participant must provide an Individual with access to PII within thirty (30) calendar days of request. • If Participant does not provide an Individual the requested access within thirty (30) calendar days of the Individual's request, Participant must provide the Individual with a timeline establishing when the requested access will be provided. • Privacy Statement shall disclose the timeline establishing when the Individual can expect a response to their request for access. [NOTE*: TRUSTe stipulates that the access program requirements under III.C.5 pertain to the data subject. Disclosure of personal information to anyone beyond the data subject would violate TRUSTe's program requirements for both first party and third-party disclosures. As such, ID verification is required when allowing the access and correction rights*.]
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the	(III.C.5.a-h) • Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII. • Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used. • Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant • Such mechanism or process shall be clear, conspicuous, and easy to use

questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do	correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	• Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and • Participant's privacy statement shall state how access is provided. • Participant is not required to permit Individual access to Personally Identifiable Information to the extent that: o Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others; o The burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However, Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or o The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information. • If Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access. (IV.A.1.a-b) • Participant must provide an Individual with access to PII within thirty (30) calendar days of request. • If Participant does not provide an Individual the requested access within thirty (30) calendar days of the Individual's request, Participant must provide the Individual with a timeline establishing when the requested access will be provided. • Privacy Statement shall disclose the timeline establishing when the Individual can expect a response to their request for access. [NOTE: *TRUSTe stipulates that the mechanism described in III.C.5.a operate within a reasonable timeframe*.]

you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?		

ACCOUNTABILITY

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement** **(Provided by TRUSTe)**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) Contracts • Compliance with applicable industry or sector laws and regulations • Compliance with self-regulatory applicant code and/or rules • Other (describe)	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and

	principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	stored *TRUSTe Master Services Agreement* section 11(f)) • Except as otherwise provided herein with respect to TRUSTe's right to provide notice via email, all notices required to be given to Participant under this Agreement must be given in writing and delivered either in hand (in which case delivery shall be effective as of the delivery date), by certified mail, return receipt requested, postage pre-paid (in which case delivery shall be effective three (3) days after mailing), or by Federal Express or other recognized overnight delivery service (in which case delivery shall be effective the day following remittance to the delivery service), all delivery charges pre-paid, and addressed to the Designated Participant Coordinator identified under the Participant's signature block hereto. • Participant acknowledges the requirement to maintain the designated participant coordinator's email account. Participant expressly consents to receipt of notification by email of the following: (i) amendments to the program requirements as provided for under section 3(b); and (ii) notification of suspension status as provided for under the applicable program amendment. Provided that TRUSTe maintains an electronic record of sending such an email notification, participant waives any right to contest actions taken by TRUSTe under sections 3(b) and the applicable program amendment based on the assertion that the email address is not valid or operational, or that the email notification was not received. [NOTE: *TRUSTe's Master License and Service Agreement Program Amendment – Privacy Program requires the granting of authority by the participant to a named individual to manage the obligations of the privacy certification. In addition, the Master Services Agreement section 11(f)) creates a Designated Participant Coordinator responsible for all matters related to any TRUSTe certification, including but not limited to*

		the unique CBPR web seal to be administered by TRUSTe.]
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	(III.D.1.h) • How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address; (III.E.6.a) • Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the	(III.E.6.a) • Participant shall provide users with reasonable, appropriate, simple effective and timely means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.

	Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	• Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices. (III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be • Appropriate to the size of the Participant's business; and • Appropriate to the level of sensitivity of the data collected and stored [NOTE: *TRUSTe stipulates that III.E.6.a includes an explanation of any subsequent remedial action taken*.]
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the	(III.E.6.a) • Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices. (III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be

	Applicant that the existence of such procedures is required for compliance with this principle.	• Appropriate to the size of the Participant's business; and • Appropriate to the level of sensitivity of the data collected and stored (III.E.2.f) • Participant must reasonably ensure their employees are trained on participants privacy policies and procedures including how to respond to privacy-related complaints.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.D.1.j) • That collected information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the Participant mergers with or is acquired by a Third Party, or goes bankrupt;
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with	(III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially

that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code and/or rules _____ • Other (describe) _____	this principle.	equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	(III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII.

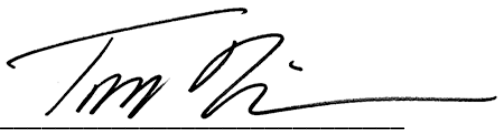
privacy practices as stated in your Privacy Statement? _____ • Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ • Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to	The Accountability Agent must verify the existence of such self-assessments.	[NOTE: *While self- assessments are not a requirement under the CBPR system for such third-parties, if used by a participant, TRUSTe agrees to verify their existence as part of the review of the steps listed under III.E.5.a.1-2.*]

ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.		(III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	(III.E.5.a.1-2) • Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII. (III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E.

		• Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	(III.E.1.a.1-2) • Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this III.E. • Such controls and processes shall be o Appropriate to the size of the Participant's business; and o Appropriate to the level of sensitivity of the data collected and stored (III.C.3.a.1) • a.Participant shall offer the Individual control over their collected Personally Identifiable Information as follows: o Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose.

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party and agrees to the findings of the Joint Oversight Panel contained herein and attests to the truth of the information provided to the Joint Oversight Panel pursuant to the Application for APEC Recognition.



[Signature of person who has authority to commit party to the agreement]

[Typed Name]: Tim Sullivan

[Date]: 19 June 2013

[Typed title]: Chief Financial officer

[Typed name of organization]: TRUSTe

[Address of organization]: 835 Market Street Suite 800, San Francisco, CA, 94103 USA

[Email address]: tims@truste.com

[Telephone number]: (415)520-3439

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.