



**Asia-Pacific
Economic Cooperation**

**APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM
REQUIREMENTS**

The purpose of this document is to provide the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to assist APEC-recognized Accountability Agents in an Applicant’s compliance review process and to ensure this process is conducted consistently throughout participating APEC Economies. Accountability Agents are responsible for receiving an Applicant’s intake documentation, verifying an Applicant’s compliance with the requirements of the CBPR System and, where appropriate, assisting the Applicant in modifying its policies and practices to meet the requirements of the CBPR System. The Accountability Agent will certify those Applicant deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Participants’ compliance with the CBPR System, based on this criteria. This document is to be read in consistently with the APEC CBPR Intake Document¹.

NOTICE..... 2

COLLECTION LIMITATION..... 6

USES OF PERSONAL INFORMNATION..... 8

CHOICE..... 11

INTEGRITY OF PERSONAL INFORMATION 15

SECURITY SAFEGUARDS 17

ACCESS AND CORRECTION 21

ACCOUNTABILITY..... 24

 GENERAL 24

 MAINTAINING ACCOUNTABILITY WHEN PERSONAL INFORMATION IS TRANSFERRED 26

¹ *NOTE:* The APEC Cross Border Privacy Rules Intake Questionnaire lists the acceptable qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms referred to in this document.

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant’s personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question	Assessment Criteria
<p>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.</p>	<p>If YES, the Accountability Agent must verify that the Applicant’s privacy practices and policy (or other privacy statement) include the following characteristics:</p> <ul style="list-style-type: none"> • 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. <p>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 justified.</p>
<p>1.a) Does this privacy statement describe how personal information is collected?</p>	<p>If YES, the Accountability Agent must verify that:</p> <ul style="list-style-type: none"> • 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. <p>If NO, the Accountability Agent must inform the Applicant that Notice as described herein is</p>

	required for compliance with this principle.
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	<p>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.</p> <p>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.</p>
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	<p>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, <u>identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.</u></p> <p>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.</p>
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.	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides name, address and a <u>functional</u> e-mail address.</p> <p>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.</p>
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	<p>Where the Applicant answers YES, the 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</p>

	Agent must verify whether the applicable qualification is justified.
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Privacy Statement includes:</p> <ul style="list-style-type: none"> • 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 <p>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 Agent must verify whether the applicable qualification is justified.</p>
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?	<p>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 <u>and that the notice is reasonably available to individuals.</u></p> <p>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.</p>
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?	<p>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.</p> <p>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 qualification, the Accountability Agent must verify whether the applicable qualification is justified.</p>
4. Subject to the qualifications listed	Where the Applicant answers YES , the Accountability Agent must verify that the Applicant

<p>below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?</p>	<p>provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes.</p> <p>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.</p>
--	---

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question	Assessment Criteria
<p>5. How do you obtain personal information:</p> <p>5.a) Directly from the individual?</p> <p>5.b) From third parties collecting on your behalf?</p> <p>5.c) Other. If YES, describe.</p>	<p>The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.</p> <p>Where the Applicant answers YES to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard.</p> <p>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.</p>
<p>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?</p>	<p>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:</p> <ul style="list-style-type: none"> • 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 with the stated purpose of collection <p>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</p> <p>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</p>

	purpose(s) for which it is collected.
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.	<p>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.</p> <p>Where the Applicant Answers NO, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.</p>

USES OF PERSONAL INFORMATION

Assessment Purpose - Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant

Question	Assessment Criteria
<p>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.</p>	<p>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.</p> <p>Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.</p>
<p>9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.</p> <p>9.a) Based on express consent of the individual?</p>	<p>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 personal information is based on express consent of the individual (9.a), such as:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page

<p>9.b) Compelled by applicable laws?</p>	<ul style="list-style-type: none"> • Via telephone • Via postal mail, or • Other (in case, specify) <p>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.</p> <p>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.</p> <p>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.</p>
<p>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.</p>	<p>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.</p>
<p>11. Do you transfer personal information to personal information processors? If YES, describe.</p>	<p>Also, the Accountability Agent must require the Applicant to identify:</p> <ol style="list-style-type: none"> 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.).
<p>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.</p>	<p>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 related purposes.</p>

<p>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?</p> <p>13.a) Based on express consent of the individual?</p> <p>13.b) Necessary to provide a service or product requested by the individual?</p> <p>13.c) Compelled by applicable laws?</p>	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>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 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.</p> <p>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.</p> <p>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.</p>
--	---

CHOICE

Assessment Purpose - Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.

Question	Assessment Criteria
<p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated.</p> <p>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 Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.</p>
<p>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?</p>	<p>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:</p>

<p>Where YES describe such mechanisms below.</p>	<ul style="list-style-type: none"> • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>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:]</p> <ul style="list-style-type: none"> • being able to make use of the personal information, when the purposes of such use is not related 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. <p>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.</p> <p>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.</p>
<p>16. 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.</p>	<p>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:</p> <ul style="list-style-type: none"> • Online at point of collection • Via e-mail

	<ul style="list-style-type: none"> • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) <p>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:</p> <ul style="list-style-type: none"> • 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.] <p>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.</p> <p>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 disclosure of their personal information must be provided.</p>
<p>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?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is displayed in a clear and conspicuous manner .</p> <p>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.</p>
<p>18. When choices are provided to the individual offering the ability to limit the</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is clearly worded and easily understandable.</p>

<p>collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?</p>	<p>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.</p>
<p>19. 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 these choices easily accessible and affordable? Where YES, describe.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant’s choice mechanism is easily accessible and affordable.</p> <p>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.</p>
<p>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.</p>	<p>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.</p> <p>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.</p> <p>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 choices, when offered, can be honored, must be provided.</p>

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question	Assessment Criteria
<p>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.</p>	<p>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.</p> <p><u>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.</u></p> <p>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.</p>
<p>22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.</p>	<p>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 <u>such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method.</u></p> <p><u>The Accountability Agent must verify that this process is in place and operational.</u></p> <p>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.</p>
<p>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</p>	<p>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</p>

<p>the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.</p>	<p>or other service providers acting on the Applicant’s behalf.</p> <p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the 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.</p>
<p>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 whom the personal information was disclosed? If YES, describe.</p>	<p>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.</p> <p>The Accountability Agent must verify that these procedures are in place and operational.</p> <p>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.</p>
<p>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-of-date?</p>	<p>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 outdated.</p> <p>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.</p> <p>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.</p>

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question	Assessment Criteria
26. Have you implemented an information security policy?	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of this written policy.</p> <p>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.</p>
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?	<p>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:</p> <ul style="list-style-type: none"> • <u>Authentication and access control (eg password protections)</u> • <u>Encryption</u> • <u>Boundary protection (eg firewalls, intrusion detection)</u> • <u>Audit logging</u> • <u>Monitoring (eg external and internal audits, vulnerability scans)</u> • <u>Other (specify)</u> <p>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 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.</p> <p>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.</p>

	<p>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.</p> <p>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.</p>
<p>28. Describe how the safeguards you identified in response to question 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.</p>	<p>Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified.</p> <p>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.</p>
<p>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).</p>	<p>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:</p> <ul style="list-style-type: none"> • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) <p>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 Applicant that the existence of such procedures are required for compliance with this principle.</p>
<p>30. Have you implemented safeguards that are proportional to the likelihood and</p>	<p>Where the Applicant answers YES (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.</p>

<p>severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:</p> <p>30.a) Employee training and management or other safeguards?</p> <p>30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?</p> <p>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?</p> <p>30.d) Physical security?</p>	<p>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.</p> <p>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.</p>
<p>31. Have you implemented a policy for secure disposal of personal information?</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information.</p> <p>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.</p>
<p>32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?</p>	<p>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.</p> <p>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.</p>
<p>33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.</p>	<p>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.</p>
<p>34. Do you use <u>risk assessments or third-party certifications</u>? Describe below.</p>	<p>The Accountability Agent must verify that such <u>risk assessments or certifications</u> are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results</p>

	<p>of these certifications or risk assessments. One example is whether 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.</p>
<p>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:</p> <p>35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?</p> <p>35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers?</p> <p>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?</p>	<p>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.</p>

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question	Assessment Criteria
<p>36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests.</p> <p>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.</p> <p>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.</p> <p>The personal information must be provided to individuals in an easily comprehensible way.</p> <p>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.</p> <p>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 the Applicant identifies an</p>

	applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
<p>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.</p> <p>37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.</p> <p>37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.</p> <p>37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.</p> <p>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)?</p> <p>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.</p>	<p>Where the Applicant answers YES the Accountability Agent must verify each answer provided.</p> <p>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.</p> <p>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.</p> <p>Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be 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.</p>
38. Do you permit individuals to challenge the accuracy of their information, and to	Where the Applicant answers YES to questions 38.a , the Accountability Agent must verify that

<p>have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).</p> <p>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.</p> <p>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?</p> <p>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?</p> <p>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?</p> <p>38.e) If access or correction is refused, do 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?</p>	<p>such policies are available and understandable in the primarily targeted economy.</p> <p>If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.</p> <p>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.</p> <p>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.</p>
---	--

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question	Assessment Criteria
<p>39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.</p> <ul style="list-style-type: none"> • 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) _____ 	<p>The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.</p>
<p>40. Have you appointed an individual(s) to be responsible for your overall compliance</p>	<p>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</p>

with the Privacy Principles?	<p>Principles.</p> <p>The Applicant must designate an individual or individuals to be responsible for the Applicant’s overall compliance with privacy 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.</p> <p>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.</p>
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	<p>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:</p> <ol style="list-style-type: none"> 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). <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	<p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.</p>
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	<p>The Accountability Agent must verify that the Applicant indicates what remedial action is considered.</p>
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including	<p>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.</p>

<p>how to respond to privacy-related complaints? If YES, describe.</p>	<p>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 Applicant that the existence of such procedures is required for compliance with this principle.</p>
<p>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?</p>	<p>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.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.</p>
<p>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 that your obligations to the individual will be met (check all that apply)?</p> <ul style="list-style-type: none"> • 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) _____ 	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of each type of agreement described.</p> <p>Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.</p>
<p>47. Do these agreements generally require that personal information processors, agents, contractors or other service</p>	<p>The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.</p>

<p>providers:</p> <ul style="list-style-type: none"> • 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 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) _____ 	
<p>48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.</p>	<p>The Accountability Agent must verify the existence of such self-assessments.</p>
<p>49. Do you carry out regular spot checking</p>	<p>Where the Applicant answers YES, the Accountability Agent must verify the existence of the</p>

<p>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.</p>	<p>Applicant's procedures such as spot checking or monitoring mechanisms.</p> <p>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.</p>
<p>50. Do you disclose personal information to other recipient <u>persons or organisations</u> 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?</p>	<p>If YES, the Accountability Agent must ask the Applicant to explain:</p> <p>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and</p> <p>(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.</p>