# Annex C

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 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:<br>• 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).<br>• Is in accordance with the principles of the APEC Privacy Framework;<br>• Is easy to find and accessible.<br>• Applies to all personal information; whether collected online or offline.<br>• States an effective date of Privacy Statement publication.<br>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. | **1.3 (Privacy policy)**<br>Privacy policy (personal information protection policy) of the applicant business entity published on its website shall fulfill the following conditions.<br><br>(1). It defines the concept of personal information protection of the entity, and the content thereof is appropriate.<br>(2). It indicates matters related to the appropriate acquisition, use, and provision of personal information considering the content and the business size (including matters related to not handling personal information beyond the scope necessary to achieve the intended purpose of use; hereafter referred to as "use other than for intended purposes"), and the content thereof is appropriate.<br>It includes provisions that are in accordance with the nine principles of the APEC Privacy Framework.<br>(3). It indicates the strict abidance by laws, guidelines and other codes stipulated by the state regarding the handling of personal information, and the content thereof is appropriate.<br>(4). It indicates how to prevent leakage, loss, and damage of personal information and correction of the same, and the content thereof is appropriate.<br>(5). It indicates how to respond to complaints and consultations, and the content thereof is appropriate.<br>(6). It indicates matters related to the continual improvement of a personal information protection management system of the entity, and the content thereof is appropriate.<br>(7). It indicates the name of the relevant representative, and the content thereof is appropriate.<br>(8). It indicates the date of enactment, and the date of enactment (including the date of the latest revision) is indicated in the personal information protection policy published on its website.<br>(9). It stipulates that measures shall be taken so that information on the personal information protection policy is available to employees and the general public; and the measures are taken. The measures shall fulfill the following conditions.<br>-When published on its website, there is a link to the personal information protection policy on the top page.<br>-Contact information for inquiries about personal information protection is indicated in the published personal information protection policy.<br>-The published personal information protection policy is identical to that described in the regulations of the entity. |
| 1.a) Does this privacy statement describe how personal information is collected? | If **YES**, the Accountability Agent must verify that:<br>• The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant.<br>• the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and<br>• The Privacy Statement reports the categories or specific sources of all categories of personal information collected.<br>If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br>The applicant business entity, when acquiring personal information with documentation directly from a person, shall describe clearly the matters described below in writing beforehand and acquire consent of the individual.<br><br>(1). In cases of direct acquisition of new types of personal information with documentation from an individual, procedure for approval of such direct acquisition; and the approval is obtained from a manager in charge in accordance with the procedure.<br>(2). Procedure for each acquisition method in which the individual is informed of the matters in a) to h) below with documentation and consent is obtained; and the business is conducted accordingly.<br>a) Name or nomenclature of the business entity<br>b) Name or title, section, and contact information of the personal information protection manager (or his/her alternate)<br>c) Purpose of use of personal information<br>d) Matters when it is planned to provide personal information to a third party<br>-Purpose for provision to the third party<br>-Items of personal information to be provided<br>-Means or method for provision<br>-Recipient of the information, or type and attributes of organization of the recipient<br>-When there is an agreement regarding the handling of personal information, the effect thereof<br>e) When entrustment of personal information handling is planned, the effect thereof<br>f) In cases of notice of the purpose of use, disclosure, correction, addition, or deletion of personal information subject to disclosure, or the right to refuse use or provision, the effect of response to the request and the person to contact for such inquiries<br>g) Voluntary nature of the individual's provision of personal information and, when the individual does not |

| | | |
|---|---|---|
| | | provide personal information, consequences to such person<br>h) When personal information is acquired by means that the individual cannot easily recognize, the effect thereof<br>(3). Cases in which consent of the individual is not required are limited only to any of (3) a) to (3) d) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" or any of (4) a) to(4) d) of "3.6 Measures concerning use."<br>(4). Procedure for approval of the cases stipulated in (3) above, and the business is conducted accordingly with approval of a manager in charge.<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br>The applicant business entity, when acquiring personal information by methods other than direct acquisition with documentation shall inform the individual of the purpose of use promptly, or publicly announce it unless the purpose of use is publicly announced beforehand. The following conditions related to such acquisition of personal information shall be fulfilled.<br><br>(1). In cases of acquisition of new types of personal information through methods other than direct acquisition with documentation, procedure for approval of such acquisition is established; and the approval is obtained from a manager in charge in accordance with the procedure.<br>(2). In cases of acquisition of personal information through methods other than direct acquisition with documentation, procedure for publicly announcing the purpose of use beforehand, or stipulate the procedure for informing the individual of the purpose of use or publicly announcing it immediately after acquisition are established;, and the business is conducted accordingly in these cases.<br>(3). Always notify the individual or make an announcement except in the cases prescribed in a) to d) below; and the business is conducted accordingly.<br>a) Cases in which informing the individual of the purpose of use or publicly announcing it may harm the life, body, property, or other rights or interests of the individual or a third party.<br>b) Cases in which informing the individual of the purpose of use or publicly announcing it may harm the rights or legitimate interests of the entity.<br>c) Cases in which the entity cooperates with a governmental institution or a local public body when executing activities prescribed by law and in which informing the individual of the purpose of use or publicly announcing it may disturb the execution of such activities.<br>d) Cases in which it is regarded that the purpose of use is clear in view of the circumstances of the acquisition.<br>(4). In cases of application of any of a) to d) above, procedure for approving such application is established, and the business is conducted accordingly.<br>(5). Application of the cases d) above is restricted in accordance with the regulation of the entity; and the business is conducted accordingly. |
| 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.<br>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. | **1.3 (Privacy policy)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.<br><br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |
| 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.<br>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.<br>Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified. | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |

| | | |
|---|---|---|
| 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.<br>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. | **1.3 (Privacy policy)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br>The applicant business entity shall configure the personal information subject to disclosure in a condition that it is readily accessible by the individual, or response is given without delay at the request of the individual. The following conditions regarding the issue shall be fulfilled.<br><br>(1). Concrete procedure for making the matters described below in a) to f) readily accessible by the individual is established, and the business is conducted accordingly.<br>a) Name of the applicant business entity and a person to contact for resolution of complaints<br>b) Name or title, section, and contact information of the personal information protection manager (or his/her alternate)<br>c) Purpose of use of all of personal information subject to disclosure<br>d) Person to contact for complaints regarding handling of personal information subject to disclosure<br>e) Name of the authorized personal information protection organization and person to contact for resolution of complaints<br>f) Procedure for responding to requests for disclosure and other requests |
| 1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information? | 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 Agent must verify whether the applicable qualification is justified. | **1.3 (Privacy policy)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.d) |
| 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:<br>• The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means).<br>• The process that an individual must follow in order to correct his or her personal information<br>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. | **5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br>The applicant business entity shall establish a procedure including the following items to respond to requests for disclosure and other requests regarding personal information.<br><br>a) Person to contact for the requests for disclosure and other requests regarding personal information are submitted<br>b) Form of documentation to be submitted when making the requests for disclosure and other requests regarding personal information, and other methods for making the requests<br>c) Method for confirming that the individual who makes a request for disclosure and other requests is the individual to whom the personal information belongs to or his/her alternate<br>d) Method for collecting charges in cases of disclosure, correction, addition, or deletion of personal information<br><br>The applicant business entity shall make sure, upon establishing the procedure for responding to requests for disclosure and other requests, that such procedure does not impose an excessive burden on the requesting individual and the requested information must be provided to individuals in an easily comprehensible way.<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.d)<br><br>**5.6 (Correction, addition, or deletion of personal information subject to disclosure)**<br>When correction, addition, or deletion of personal information subject to disclosure is requested from an individual claiming that content of the personal information is unfounded, except in cases in which there is any legal basis, the applicant business entity shall execute a necessary investigation without delay within the scope of the purpose of use, and make corrections, etc. The following conditions regarding the issue shall be fulfilled.<br><br>(1). The applicant business entity established regulations to execute the necessary investigation without delay within the scope necessary for achievement of the purpose of use and make a correction, etc. based on the result when correction, etc., of personal information subject to disclosure that leads to the identification of the |

| | | |
|---|---|---|
| | | individual is requested by an individual, except when a special procedure is stipulated by relevant law, and the business is conducted accordingly.<br>(2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure.<br>(3). Procedure for approving not to make a correction, etc. is established, and approval of a manager in charge is obtained when personal information is not corrected, etc. |
| 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.<br>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. | **1.3 (Privacy policy)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.<br><br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |
| 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.<br>Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organizations, 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. | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |
| 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.<br>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. | |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 5. How do you obtain personal information:<br>5.a) Directly from the individual?<br>5.b) From third parties collecting on your behalf?<br>5.c) Other. If YES, describe. | The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information.<br>Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard.<br>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. | **3.2 (Appropriate acquisition of personal information)**<br>The applicant business entity shall acquire personal information by fair and lawful means. The following conditions related to the acquisition of personal information shall be fulfilled.<br><br>(1). Acquisition of personal information is carried out in a fair and lawful manner in accordance with the regulation of the entity; and the business of the entity is conducted accordingly.<br>(2). In the case of acquiring personal information from any person other than the individual, including in cases of entrustment, the entity confirms, in accordance with the regulation of the entity, that a provider or trustee handles personal information in an appropriate manner; and the business of the entity is conducted accordingly to confirm that personal information is handled by the provider or trustee in accordance with the procedure. |

| | | |
|---|---|---|
| | | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |
| 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:<br>• Each type of data collected<br>• The corresponding stated purpose of collection for each; and<br>• All uses that apply to each type of data<br>• An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection<br>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<br>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.。 | **2.1 (Identification of personal information)**<br>The applicant business entity shall establish and maintain a procedure for identifying all of the personal information that the entity uses for the business. The procedure shall fulfill the following conditions.<br><br>(1). Procedure for identifying every piece of personal information is provided clearly.<br>(2). Personal information is identified in accordance with the aforementioned procedure, and approval is obtained from a manager in charge.<br>(3). Records, etc. for identifying personal information is maintained.<br>(4). Procedure for updating and periodic review of the records, etc. of personal information identification is provided clearly.<br>(5). Updating and periodic review of the records, etc. of personal information identification are conducted in accordance with the aforementioned procedure.<br><br>**3.1 (Identification of the purpose of use)**<br>The applicant business entity, when acquiring personal information, shall identify the purpose of use insofar as is possible, and use personal information within the scope of such purpose. The following conditions related to the identification of the purpose of use shall be fulfilled.<br><br>(1). Upon acquisition of personal information, the purpose of use thereof is identified to the greatest possible extent, and personal information is used within the scope necessary for the achievement of the purpose, in accordance with the regulation of the entity; and the business of the entity is conducted accordingly.<br>(2). Procedure for identifying the purpose of use is established, and approval is obtained from a manager in charge when identifying the purpose of use.<br>(3). Employees of the entity that handles personal information recognize clearly the purpose of use.<br><br>**3.6 (Measures concerning use)**<br>The applicant business entity shall use the personal information within the scope necessary for the achievement of the identified purpose of use. When using personal information beyond the scope necessary for the achievement of the identified purpose of use, the entity shall inform the person of matters equivalent to or more satisfactory than those provided upon direct acquisition of personal information with documentation from the individual in content, and obtain consent of the person. The following conditions related to the measures concerning use shall be fulfilled.<br><br>(1). Personal information is utilized within the scope necessary for the achievement of the identified purpose of use in accordance with the regulation of the entity; and the business is conducted accordingly.<br>(2). Procedure for approving changes in the purpose of use is established; and the business is conducted accordingly.<br>(3). Procedures for informing the individual of the matters stipulated in (2) a) to (2) f) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content upon making changes in the purpose of use and for obtaining consent of such person are established, and the business is conducted accordingly.<br>(4). Use other than for intended purposes that does not require the consent of the individual is limited exclusively to the cases in a) to d) below, and the business is conducted accordingly.<br>a) Cases in which the use of personal information is required by a law.<br>b) Cases in which the use of personal information is necessary for the protection of the life, body, or property of an individual, and in which it is difficult to acquire the consent of the individual.<br>c) Cases in which the use of personal information is especially necessary to improve public hygiene or promote the sound growth of children and in which it is difficult to acquire the consent of the individual.<br>d) Cases in which the use of personal information is necessary for cooperating with a governmental institution or a local public body when executing activities prescribed by law and in which acquiring the consent of the individual may disturb the execution of such activities. |

| | | |
|---|---|---|
| | | (5). In cases of application of any of a) to d) above, procedure for approving such application is established; and the business is conducted accordingly.<br>(6). When it is found difficult to determine whether or not a case falls under the use other than for intended purposes, a manager in charge is requested to determine the same in accordance with the regulation of the entity; and the business is conducted accordingly. |
| 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.<br>Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle. | **2.2 (Laws, guidelines, and other codes stipulated by the state)**<br>The applicant business entity shall establish a procedure and management system for identifying and referring to laws, guidelines, and other codes stipulated by the government of Japan regarding the handling of personal information including responding to judicial or other government subpoenas, warrants and orders. The procedure and management system shall fulfill the following conditions<br><br>(1). Procedure for identifying, referring to, and maintaining laws, guidelines, and other codes stipulated by the government of Japan related to the handling of personal information is established.<br>(2). Laws, guidelines, and other codes that need to be referenced are identified in accordance with the aforementioned procedure, and updated as necessary with approval of a manager in charge.<br>(3). Identified laws, guidelines, and other codes that need to be referenced are appropriate.<br>(4). Identified laws, guidelines, and other codes that need to be referenced are made available for reference as necessary and such references are required to include appropriate procedures to handle inquiries, requests, etc. from abroad.<br><br>**3.2 (Appropriate acquisition of personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 5. |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 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.<br>Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below. | **2.5 (Internal regulations)**<br>The applicant business entity shall have detailed regulations which cover items (1) to (15) below. These regulations shall be determined in accordance with its formal internal procedures, and they shall be available for reference to all employees.<br><br>(1). Procedure for identifying personal information<br>(2). Procedure for identification, reference, and maintenance of laws, guidelines, and other codes stipulated by the government of Japan.<br>(3). Procedure for recognizing and analyzing risks related to personal information and taking relevant measures<br>(4). Authority and responsibility to protect personal information in each section and at each level of the entity<br>(5). Preparation for states of emergency and responses thereto (when leakage, loss, or damage of personal information occurs)<br>(6). Acquisition, use, and provision of personal information<br>(7). Appropriate management of personal information<br>(8). Response to a request for disclosure and other matters from individual<br>(9). Training of staff members<br>(10).Management of documents of the personal information protection management system<br>(11).Responses to complaints and consultations<br>(12).Internal inspection<br>(13).Corrective action and preventative action<br>(14).Review by the representative<br>(15).Punitive provisions for violation of the internal regulations<br><br>**3.1 (Identification of the purpose of use)**<br>Reshown, see "Relevant Program Requirement" of Question 6.<br><br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.6 (Measures concerning use)**<br>Reshown, see "Relevant Program Requirement" of Question 6. |
| 9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.<br>9.a) Based on express consent of the individual?<br><br>9.b) Compelled by applicable | 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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.6 (Measures concerning use)**<br>Reshown, see "Relevant Program Requirement" of Question 6. |

| | | |
|---|---|---|
| laws? | • Via postal mail, or<br>• Other (in case, specify)<br>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.<br>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.<br>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. | |
| 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.<br><br>11. Do you transfer personal information to personal information processors? If YES, describe.<br><br>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. | 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.<br>Also, the Accountability Agent must require the Applicant to identify:<br>1) each type of data disclosed or transferred;<br>2) the corresponding stated purpose of collection for each type of disclosed data; and<br>3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.).<br>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. | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.8 (Measures concerning provision of personal information)**<br>The applicant business entity, when providing a third party with personal information, shall inform the individual of the acquisition method and matters equivalent to or more satisfactory than the matters stipulated in (2) a) to (2) d) of "3.4 Measures for acquiring personal information with documentation directly from the individual" in content beforehand, and obtain the consent of the person. The following conditions related to the measures concerning provision of personal information shall be fulfilled.<br><br>(1). In cases in which personal information is provided to a third party, procedure for approving such provision is established, and the business is conducted accordingly.<br>(2). In cases in which personal information is provided to a third party, procedures for informing the individual of the acquisition method and matters stipulated in (2) a) to (2) d) of "3.4 Measures for acquiring personal information with documentation directly from the individual" or matters equivalent to or more satisfactory than such matters in content beforehand, and for obtaining the consent of such person are established, and the business is conducted accordingly.<br>(3). In cases in which personal information is provided beyond the scope necessary for the achievement of the identified purpose of use, consent of the person is obtained in accordance with the procedure for use other than for intended purposes stipulated in (3) of "3. 6 Measures concerning use."<br>(4). Always require the consent of the person except in the cases in a) to f) below, and the business is conducted accordingly.<br>a) When it is difficult to acquire the consent of the person as the business entity provides a large amount of personal information widely to the public, and in case the business entity informs the individual of the matters described below or matters equivalent to or more satisfactory than such matters in content beforehand, or other equivalent alternative measures are taken.<br>-The fact that provision to the third party is the purpose of use<br>-Items of personal information provided to the third party<br>-Measures or method of provision to the third party<br>-The fact that provision of personal information that could lead to identification of the individual to the third party will be stopped in accordance with a request from the individual<br>-Acquisition methods of the personal information<br>b) In a case in which information regarding executives and stockholders of a corporation or organization included in information regarding the corporation or organization is provided, and the information is provided based on laws or disclosed or publicly announced voluntarily by the person or the corporation or organization; when the business entity informs the individual of the matters described in a) above or matters equivalent to or more satisfactory than that in content beforehand, or makes information on such matters readily accessible to the individual<br>c) When the business entity entrusts all or part of the handling of personal information within the scope necessary for the achievement of the identified purpose of use<br>d) In a case in which personal information is provided with succession of business because of mergers or other reasons, and when the personal information is handled within the scope of the purpose of use before the |

| | | |
|---|---|---|
| | | business succession<br>e) When personal information is used jointly by specific entities, and in case the business entity informs the individual of the matters described below or matters equivalent to or more satisfactory than such matters in content beforehand, or makes information on such matters readily accessible to the individual.<br>-The fact that the personal information will be used jointly<br>-Items of the personal information jointly used<br>-Scope of the joint users<br>-Purpose of use of the joint users<br>-Name or nomenclature of a person who has responsibility for controlling the personal information jointly used<br>-Acquisition methods of the personal information jointly used<br>f) When any of (4) a) to d) of the proviso of "3.6 (measures concerning use)" can be applied.<br>(5). In cases of application of any of a) to f) above, procedure for approving such application is established, and the business is conducted accordingly.<br>(6). In cases in which a) above is applied, procedures for notifying the individual of each sub-item in advance, or taking alternative equivalent measures are established, and the business is conducted accordingly.<br>(7). In cases in which b) above is applied, procedures for notifying the individual of the matters described in a) or matters equivalent to or more satisfactory than such matters in content beforehand, or making information on such matters readily accessible to the individual are established, and the business is conducted accordingly.<br>(8). In cases in which e) above is applied, procedure therefor is established, and the business is conducted accordingly.<br><br>**4.2 (Security control measures for personal information)**<br>The applicant business entity, as shown below I and II, shall take necessary and appropriate measures to prevent leakage, loss, and damage of personal information, and other security control measures for personal information, according to the risk of the personal information to be handled.<br><br>I. Measures that should be taken as physical security control measures<br>(1). Entrance/exit control<br>a) Entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are restricted.<br>b) Records of entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are made and maintained.<br>c) Records of entrance to and exit from the buildings, rooms, server rooms, and places in which personal information is handled are periodically checked.<br>(2). Antitheft control<br>a) Documents, media, portable computers, etc., on which personal information is contained are not left on the desk when the person in charge is not at the desk.<br>b) Each computer with which personal information is handled is logged off or a screensaver with a password is launched whenever the person in charge leaves his/her computer.<br>c) Any media (papers and recording media) on which personal information is recorded are kept under lock and key.<br>d) Keys to the storage places for media on which personal information is recorded are in the custody of a person in change.<br>e) Any media (papers and recording media) on which personal information is recorded are made unusable when they are disposed of.<br>f) Antitheft measures are applied to portable computers, etc., on which personal information is recorded.<br>g) Rules are established and followed with regard to the use of portable computers and external storage media such as, USB flash memory, and CD-ROM.<br>h) Operation manuals for information systems with which personal information is handled are not left on desks.<br>(3). Physical protection of equipment and devices, etc.<br>a) Equipment and devices, etc., with which personal information is handled are physically protected from security risks (including theft, disposal, and breakage) as well as environmental risks (including water leaks, fire, power failures, and earthquakes).<br><br>II. Measures that should be taken as technical security control measures<br>(1). Identification and authentication with respect to access to personal information<br>a) Authentication using identification data (username, password, etc.) is performed in order to control access to personal information.<br>b) Default settings for information systems on which personal information is stored are properly changed as |

| | | |
|---|---|---|
| | | necessary.<br>c) Issuance, updating, and disposal of identification data are taking place in accordance with the rules.<br>d) Identification data is not stored in plain text.<br>e) Setting and use of identification data are taking place in accordance with the rules.<br>f) Use of terminals and addresses, etc., for employees having access rights to personal information is restricted.<br>(2). Control of access to personal information<br>a) The number of employees who have access to personal information is kept to a bare minimum.<br>b) Identification data for accessing personal information is not shared with more than one person.<br>c) Access rights granted to employees are kept to a bare minimum.<br>d) The number of simultaneous users of an information system on which personal information is stored is limited.<br>e) Utilization time of the information systems on which personal information is stored is limited.<br>f) Information systems on which personal information is stored are protected against unauthorized access.<br>g) Unauthorized use of applications which enables accessing to personal information is prevented.<br>h) Effectiveness of the access control functions introduced to the information systems for handling personal information has been verified.<br>(3). Control of access rights to personal information<br>a) Control of rights to give permission to persons to access personal information is performed appropriately on a regular basis.<br>b) Access to information systems for handling personal information is controlled by being kept to a bare minimum.<br>(4). Records of access to personal information<br>a) Records of access to personal information and of the success or failure of such operations are acquired and maintained.<br>b) Acquired records are appropriately protected against leaks, loss, and damage.<br>(5). Protection measures against malware for information systems handling personal information<br>a) Antivirus software is installed in the information system.<br>b) Security-fix programs (or security patches) for the operating systems and applications are applied.<br>c) Effectiveness and stability of the protection measures against malware are confirmed.<br>d) File-sharing software (such as Winny, Share, and Cabos) is not installed in terminals from which access to personal information is possible.<br>(6). Measures at the time of transfer and communication of personal information<br>a) Records of giving and receiving personal information are maintained upon transfer of personal information.<br>b) Measures are established in case a recording medium containing personal information is lost or stolen during transfer.<br>c) Personal information being transmitted through a network that is vulnerable to sniffing (e.g. internet and wireless LAN) is encrypted or password-locked for security purposes.<br>(7). Measures when checking the operations of information systems for handling personal information<br>a) Personal information is not used as test data when checking the operations of the information systems.<br>b) When changes are made in the information systems, it is confirmed that the level of security of the information systems and the operational environment are not decreased thereby.<br>(8). Monitoring of information systems for handling personal information<br>a) Usage of the information systems for handling personal information is periodically checked.<br>b) Status of access to personal information (including operation details) is periodically checked.<br><br>**4.4 (Supervision of trustees)**<br>The applicant business entity, when entrusting handling of personal information, shall establish criteria for selecting trustees and select trustees who satisfy the requirements for the sufficient protection level that is the same as or higher than the protection level of the applicant business entity.(*The term "trustees" here includes processors, agents, contractors or other service providers who are entrusted to handle personal information.)<br><br>(1). Procedure for establishing and reviewing criteria for selecting trustees is established, and concrete and feasible criteria for selecting trustees is set in place accordingly.<br>(2). Review of the criteria for selecting trustees is conducted as necessary.<br>(3). Trustees are evaluated based on the criteria for selecting trustees (including periodical reevaluations) in accordance with the regulation of the entity, and the business is conducted accordingly.<br>(4). All relevant trustees are recognized.<br>(5). Procedure for concluding a contract that includes the content of a) to g) below is established, and the business is conducted accordingly.<br>a) Clarification of responsibilities of the trustor and trustee |

| | | |
|---|---|---|
| | | b) Matters regarding security control of personal information<br>c) Matters regarding re-entrusting<br>d) Content and frequency of reports about the handling status of personal information to the trustor<br>e) Matters that enable the trustor to confirm that the content of the agreement is observed<br>f) Measures in case the content of the agreement is not observed<br>g) Matters regarding report and communication to the trustor when an incident or an accident occurs<br>(6). Procedure for retaining the relevant documents including the above said contract for the personal information retention period is established, and the business is conducted accordingly. |
| 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?<br>13.a) Based on express consent of the individual?<br>13.b) Necessary to provide a service or product requested by the individual?<br>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.<br>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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br>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.<br>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.<br>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. | **2.2 (Laws, guidelines, and other codes stipulated by the state)**<br><br>Reshown, see "Relevant Program Requirement" of Question 7.<br><br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.5 (Measures for acquiring personal information by methods other than direct acquisition with documentation )**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br><br>**3.6 (Measures concerning use)**<br><br>Reshown, see "Relevant Program Requirement" of Question 6.<br><br>**3.8 (Measures concerning provision of personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |

**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 (*to be answered by the Applicant*)** | **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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br>The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated.<br>Where the Applicant answers **NO**, the Applicant must identify the applicable qualification | **1.2 (Option for the individual)**<br>The applicant business entity shall make the acquisition, use and disclosure of personal information optional for the individual.<br><br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.a) |

| | | |
|---|---|---|
| | and the Accountability Agent must verify whether the applicable qualification is justified.<br>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. | |
| 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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br>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.<br>Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:<br>• 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<br>• Personal information may be disclosed or distributed to third parties, other than Service Providers.<br>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.<br>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. | **1.2 （Option for the individual）**<br>Reshown, see "Relevant Program Requirement" of Question 14.<br>**3.4 （Measures for acquiring personal information with documentation directly from the individual）**<br>Reshown, see "Relevant Program Requirement" of Question 1.a）<br>**3.6 （Measures concerning use）**<br>Reshown, see "Relevant Program Requirement" of Question 6.<br>**3.8 （Measures concerning provision of personal information）**<br>Reshown, see "Relevant Program Requirement" of Question10-12.<br>**5.2 （Procedure for satisfying the rights of the individual concerning personal information）**<br>Reshown, see "Relevant Program Requirement" of Question 1.f） |
| 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. | 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:<br>• Online at point of collection<br>• Via e-mail<br>• Via preference/profile page<br>• Via telephone<br>• Via postal mail, or<br>• Other (in case, specify)<br>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.<br>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:<br>• 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.]<br>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.<br>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. | **1.2 （Option for the individual）**<br>Reshown, see "Relevant Program Requirement" of Question 14.<br>**3.4 （Measures for acquiring personal information with documentation directly from the individual）**<br>Reshown, see "Relevant Program Requirement" of Question 1.a）<br>**3.5 （Measures for acquiring personal information by methods other than direct acquisition with documentation ）**<br>Reshown, see "Relevant Program Requirement" of Question 1.a）<br>**3.8 （Measures concerning provision of personal information）**<br>Reshown, see "Relevant Program Requirement" of Question 10.-12.<br>**5.2 （Procedure for satisfying the rights of the individual concerning personal information）**<br>Reshown, see "Relevant Program Requirement" of Question 1.f） |
| 17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or | Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner .<br>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 | **1.2 （Option for the individual）**<br>Reshown, see "Relevant Program Requirement" of Question 14. |

| | | |
|---|---|---|
| disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner? | 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. | **3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br>**3.8 (Measures concerning provision of personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 10.-12.<br>**5.1 (Rights of the individual concerning personal information)**<br>Concerning personal information regarding which the applicant business entity has the authority to respond to all requests for the disclosure, correction of content, addition or deletion, stopping use, erasing, and stopping provision to a third party thereof made by the individual, in cases in which such personal information is composed systematically and constituted so as to allow retrieval of specific pieces of information by computers (hereafter referred to as "personal information subject to disclosure"), the business entity shall respond to such requests within one month, in principle, and if it cannot respond to them within one month, it shall inform the individual of the status and reason. The following conditions related to the rights of individual concerning personal information shall be fulfilled.<br>(1). The business entity established regulations to respond to requests for disclosure and other requests regarding personal information subject to disclosure by the individual, and the business is conducted accordingly.<br>(2). There are no omissions in personal information subject to disclosure.<br>(3). Items exempted from the category of personal information subject to disclosure are limited to cases in the exceptional provisions.<br>(4). Procedure for approving the application of the exceptional provisions is established, and the business is conducted accordingly.<br>**5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 1.f) |
| 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.<br>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. | |
| 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. | Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable.<br>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. | |
| 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.<br>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.<br>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. | **1.2 (Option for the individual)**<br>Reshown, see "Relevant Program Requirement" of Question 14.<br>**3.4 (Measures for acquiring personal information with documentation directly from the individual)**<br>Reshown, see "Relevant Program Requirement" of Question 1.a)<br>**5.1 (Rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 17-19.<br>**5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 1.f)<br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br>Reshown, see "Relevant Program Requirement" of Question 1.d)<br>**5.4 (Notification regarding purpose of use of personal information subject to disclosure)**<br>When notification of purpose of use is requested from an individual concerning personal information subject to disclosure that leads to identification of the individual, the applicant business entity shall respond thereto without delay. However, when any of (3) a) to (3) c) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" is applied, or when the purpose of use of personal information subject to disclosure which leads to the identification of the individual is clear in accordance with (1) c) of "5.3 Making the matters concerning personal information subject to disclosure widely known," it is not necessary to inform the individual of the purpose of use, while the business entity shall inform the individual to such effect without delay and explain the relevant reason. The following conditions regarding the issue shall be fulfilled. |

| | | |
|---|---|---|
| | | (1). The applicant business entity establishes regulations to respond without undue delay when notification of the purpose of use is requested by an individual, and the business is conducted accordingly.<br>(2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated.<br>(3). Notification regarding the purpose of use is always provided except for the cases stipulated above.<br>(4). Procedure for approving not to notify the purpose of use according to the exceptional provisions stipulated above is established, and the business is conducted accordingly.<br><br>**5.5 (Disclosure of personal information subject to disclosure )**<br>When disclosure of personal information is requested from an individual concerning personal information subject to disclosure that leads to identification of the individual, unless there are any relevant laws prohibiting the disclosure, the applicant business entity shall disclose the personal information subject to disclosure without delay via document to the individual. However, when any of a) to c) given below is applicable upon disclosure, it is not necessary to disclose all or part of the relevant information, while the business entity shall inform the individual to such effect without delay and explain the relevant reason.<br><br>a) Cases in which disclosure may harm the life, body, property, or other rights or interests of the individual or a third party<br>b) Cases in which disclosure may seriously disturb the appropriate execution of the business of the business entity<br>c) Cases in which disclosure violates relevant law<br><br>The following conditions regarding the issue shall be fulfilled.<br><br>(1). The applicant business entity establishes regulations to respond without undue delay when disclosure of personal information subject to disclosure that leads to the identification of the individual is requested by an individual, except when a special procedure is stipulated by relevant law and the business is conducted accordingly.<br>(2). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure.<br>(3). Response to a request for disclosure is always provided except for the cases stipulated in a) to c) above.<br>(4). Procedure for approving not to disclosure all or part of the relevant information according to the exceptional provisions stipulated above is established, and the business is conducted accordingly. |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 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.<br>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.<br>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. | **4.1 (Securement of accuracy of personal information)**<br>The applicant business entity shall maintain personal information correct and in an up-to-date state, within the scope of the purpose of use. The following conditions related to the maintenance of personal information shall be fulfilled.<br><br>(1). Procedure for enabling reference and confirmation upon input of personal information<br>a) Person in charge of inputting personal information is clearly indicated.<br>b) Procedure for enabling reference to and confirmation of inputted personal information is clearly indicated.<br>c) Referencing and confirmation work are conducted in accordance with the procedure.<br>(2). Procedure for data correction<br>a) Person in charge of correcting personal information data is clearly indicated.<br>b) Procedure for discovering inaccuracy or inconsistency of corrected personal information data is clearly indicated.<br>c) Procedure for enabling reference to and confirmation of corrected personal information data is clearly indicated.<br>d) Data correction work is conducted in accordance with the procedure.<br>(3). Procedure for verifying that personal information is accurate and in an up-to-date state<br>a) Person in charge of verifying that personal information is accurate and in an up-to-date state is clearly indicated.<br>b) Procedures for verifying that personal information is accurate and in an up-to-date state and correcting it as necessary are clearly indicated.<br>c) Verification work is conducted in accordance with the procedure.<br>(4). Update of matters recorded<br>a) Person in charge of maintenance of records of conducted work is clearly indicated.<br>b) Procedure for updating records of conducted work is clearly indicated.<br>c) Procedure for keeping records of conducted work is clearly indicated.<br>d) Update of matters recorded is conducted in accordance with the procedure.<br>(5). Retention period of personal information<br>a) Person in charge of determining retention period is clearly indicated.<br>b) A criterion for determining retention period is clearly indicated.<br>c) Retention period is determined in accordance with the procedure. |
| 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. | 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 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.<br>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. | **4.1 (Securement of accuracyof personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 21.<br><br>**5.1 (Rights of the individual concerning personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 17-19.<br><br>**5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.f)<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.d)<br><br>**5.6 (Correction, addition, or deletion of personal information subject to disclosure)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.f) |

| | | |
|---|---|---|
| 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 information was transferred? 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 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.<br>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.<br>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. | **4.1 (Securement of accuracy of personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 21.<br><br>**4.4 (Supervision of trustees)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |
| 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. | 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.<br>The Accountability Agent must verify that these procedures are in place and operational.<br>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. | |
| 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? | 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.<br>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.<br>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. | |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 26. Have you implemented an information security policy? | Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy.<br>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. | **2.3 (Recognition, analysis of risk, and related measures)**<br>The applicant business entity shall establish and maintain a procedure for taking necessary measures so as not to use identified personal information other than for the intended purposes. The procedure shall fulfill the following conditions.<br><br>(1). Procedure for taking necessary measures is established and maintained so that relevant information shall not be used other than for the intended purposes; and the procedure is implemented.<br>(2). Procedures for identifying risks of identified personal information throughout its lifecycle analyzing risks taking appropriate measures to deal with these risks, and recognizing any remaining risks are established clearly; and the procedures are implemented.<br>(3). Risks of each personal information throughout its lifecycle are recognized and analyzed. Appropriate measures are taken to deal with such risks, and any remaining risks are identified clearly.<br>(4). Measures to be taken against identified risks are approved by the representative of the entity.<br>(5). Aforementioned measures are reflected in the regulations of the entity.<br>(6). Procedures for periodic review and occasional review in accordance with needs are established clearly; and the review of risks is conducted in accordance with the procedures.<br><br>**4.2 (Security control measures for personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |
| 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:<br>• Authentication and access control (eg password protections)<br>• Encryption<br>• Boundary protection (eg firewalls, intrusion detection)<br>• Audit logging<br>• Monitoring (eg external and internal audits, vulnerability scans)<br>• Other (specify)<br>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.<br>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.<br>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.<br>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. | |
| 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. | 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.<br>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. | |
| 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:<br>• Training program for employees<br>• Regular staff meetings or other communications<br>• Security policy signed by employees<br>• Other (specify)<br>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. | **2.3 (Recognition, analysis of risk, and related measures)**<br><br>Reshown, see "Relevant Program Requirement" of Question 26.-28.<br><br>**4.2 (Security control measures for personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10-12.<br><br>**4.3 (Supervision of employees)**<br>The applicant business entity, when making its employees handle personal information, shall supervise the employees in an appropriate manner and to the extent necessary to ensure security control measures of the personal information. The following conditions related to the supervision of employees shall be fulfilled. |

| | | |
|---|---|---|
| | | (1). Regulation to conduct necessary and appropriate supervision of the employees is established, and the business is conducted accordingly.<br>(2). Non-disclosure agreement with respect to personal information is signed with each employee at the start of employment contract or entrustment contract in accordance with the regulation of the entity, and the business is conducted accordingly.<br>(3). At the start of employment contract or entrustment contract, etc., the non-disclosure provision is made valid for a certain period even after the termination of the contract in accordance with the regulation of the entity, and the business is conducted accordingly.<br>(4). Regulations regarding measures to deal with cases of breaches of the personal information protection management system is established, and the business is conducted accordingly.<br>(5). In cases of monitoring of employees using a video or online, implementation measures of such monitoring are established, and the business is conducted accordingly.<br>(6). Regulations concerning a person in charge of the monitoring and his/her authority are established, and the business is conducted accordingly.<br>(7). Regulations concerning the monitoring are established and shared throughout the entity beforehand; and audit or confirmation with regard to proper implementation of the monitoring is conducted.<br><br>**6.(Training of employees)**<br>The applicant business entity shall periodically provide employees with appropriate training, and establish and maintain a procedure for making employees understand necessary matters for each relevant function and level. The following conditions regarding the training shall be fulfilled.<br><br>(1). The applicant business entity establishes regulations to periodically provide all employees with appropriate training concerning personal information protection, and the training is provided in accordance with a training plan.<br>(2). All employees are provided with appropriate training concerning personal information protection.<br>(3). The regulation or training plan includes at least the contents of a) to c) below.<br>a) Importance and advantage of being conformity with the personal information protection management system<br>b) Role and responsibility to conform with the personal information protection management system<br>c) Results to be anticipated when the personal information protection management system is violated<br>(4). Training materials include the contents of a) to c) above.<br>(5). Procedure for checking the participants' level of understanding is established, and the business is conducted accordingly.<br>(6). Procedures for determining the responsibility and authority regarding the training plan and the implementation thereof, reporting of results of the training and their review, review of the training plan, and retention of records thereof are established, and the business is conducted accordingly. |
| 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:<br>30.a) Employee training and management or other safeguards?<br>30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?<br>30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?<br>30.d) Physical security? | Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards.<br>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.<br>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. | **2.3 (Recognition, analysis of risk, and related measures)**<br><br>Reshown, see "Relevant Program Requirement" of Question 26.-28.<br><br>**4.2 (Security control measures for personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10-12.<br><br>**4.3 (Supervision of employees)**<br><br>Reshown, see "Relevant Program Requirement" of Question 29.<br><br>**6.(Training of employees )**<br><br>Reshown, see "Relevant Program Requirement" of Question 29. |
| 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.<br>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. | **2.3 (Recognition, analysis of risk, and related measures)**<br><br>Reshown, see "Relevant Program Requirement" of Question 26.-28. |
| 32. Have you implemented | Where the Applicant answers **YES**, the Accountability Agent must verify the existence of | **2.7 (Emergency responses)** |

| | | |
|---|---|---|
| measures to detect, prevent, and respond to attacks, intrusions, or other security failures? | 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. | The applicant business entity shall establish, implement, and maintain a procedure for identifying states of emergency and responding thereto.<br>Such procedure shall be established to minimize the effects in consideration of the possibility of economic disadvantages and loss of social credibility, effects on the individual, etc., supposed in case of leakage, loss, or damage of personal information. The procedure shall fulfill the following conditions.<br><br>(1). Procedure for identifying states of emergency and responding thereto is established; and the procedure is implemented.<br>(2). Procedure for minimizing the effects in consideration of the possibility of economic disadvantages and loss of social credibility, effects on the individual, etc., supposed in case of leakage, loss, or damage of personal information, is established; and measures in accordance with the procedure are implemented.<br>(3). Procedure for ensuring that the individual is promptly informed of the content of the personal information leaked, lost, or damaged, or ensuring that the individual is easily accessible to be informed of the content thereof, is established and measures in accordance with the procedure are implemented.<br>(4). Procedure for publicly announcing facts, causes, and counter measures insofar as is possible without delay from the perspective of prevention of secondary damage and avoidance of the occurrence of similar events is established; and measures in accordance with the procedure are implemented.<br>(5). Procedure for promptly reporting on facts, causes, and counter measures to related organizations (organizations that have an interest in receiving such reports) in case of emergency is established.<br><br>**4.2 (Security control measures for personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10-12. |
| 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. | |
| 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 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. | **2.3 (Recognition, analysis of risk, and related measures)**<br><br>Reshown, see "Relevant Program Requirement" of Question 26.-28.<br><br>**4.2 (Security control measures for personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10-12.<br><br>**9.2 (Internal audit)**<br>The applicant business entity shall periodically conduct internal audit regarding the status of the conformance of its personal information protection management system with the requirements of the certification standards, and the operational status of the personal information protection management system. The following conditions regarding the internal audit shall be fulfilled.<br><br>(1). The applicant business entity establishes regulations to conduct internal audit with regard to conformance with the requirements of the certification standards and the operating status thereof , and the internal audit is implemented in accordance with an audit plan.<br>(2). Internal audit regarding the conformance and operating status is conducted at all sections of the entity.<br>(3). The applicant business entity establishes regulations to let representative of the entity appoint a person within the entity whose position is fair and objective as the personal information protection auditor, and the business is conducted accordingly.<br>(4). The applicant business entity establishes regulations to let the personal information protection auditor direct the internal audit, prepare an audit report, and submit it to representative of the entity, and the business is conducted accordingly.<br>(5). The applicant business entity establishes regulations to ensure that objectivity and fairness of the internal audit and no auditor audits a section to which he or she belongs to, and the business is conducted accordingly.<br>(6). Procedures for determining responsibility and authority regarding the audit plan and the implementation thereof are established, and the business is conducted accordingly. |
| 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 | 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. | **2.3 (Recognition, analysis of risk, and related measures)**<br><br>Reshown, see "Relevant Program Requirement" of Question 26.-28.<br><br>**2.7 (Emergency responses)**<br><br>Reshown, see "Relevant Program Requirement" of Question 32 and 33. |

| | | |
|---|---|---|
| other misuses of the information by:<br>35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?<br>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?<br>35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach? | | **4.2 (Security control measures for personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 10-12.<br><br>**4.3 (Supervision of employees)**<br>Reshown, see "Relevant Program Requirement" of Question 29.<br><br>**4.4 (Supervision of trustees)**<br>Reshown, see "Relevant Program Requirement" of Question 10-12. |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 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.<br>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.<br>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.<br>The personal information must be provided to individuals in an easily comprehensible way.<br>The Applicant must provide the individual with a time frame indicating when the requested access will be granted.<br>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 applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified. | **5.1 (Rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 17-19.<br><br>**5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 1.f) |
| 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.<br>37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.<br>37.b) Do you provide access within a reasonable time frame | Where the Applicant answers **YES** the Accountability Agent must verify each answer provided.<br>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.<br>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.<br>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. | **5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 1.f)<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br>Reshown, see "Relevant Program Requirement" of Question 1.d)<br><br>**5.5 (Disclosure of personal information subject to disclosure)**<br>Reshown, see "Relevant Program Requirement" of Question 20.<br><br>**5.7 (Veto of use or provision of personal information subject to disclosure)**<br>When stopping use of, erasing, amendment, or stopping provision to a third party of personal information subject to disclosure that leads to the identification of the individual is requested by an individual, the applicant business entity |

| | | |
|---|---|---|
| following an individual's request for access? If YES, please describe.<br>37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.<br>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)?<br>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. | | shall respond thereto. Also, the business entity, after taking relevant measures, shall inform the individual of the result providing a copy on correction of personal information including deletion and amendment without delay. However, when any of (3) a) to (3) c) of "3.5 Measures for acquiring personal information by methods other than direct acquisition with documentation" is applied, it is not necessary to execute the stopping of the use, etc. while the business entity shall inform the individual to such effect without delay and explain the relevant reason.<br><br>(1). The applicant business entity establishes regulations to respond to a request from an individual regarding stopping use, etc., of personal information subject to disclosure that leads to the identification of the individual and the business is conducted accordingly.<br>(2). The applicant business entity establishes regulations to inform the individual after taking relevant measure without delay, and the business is conducted accordingly.<br>(3). Procedure for approving the content of the reply to the individual (including cases in which the request is to be denied) is established, and such procedure is clearly indicated. Approval of a manager in charge regarding the content of the reply to the individual is obtained in accordance with the procedure.<br>(4). Response to a request for stopping the use, etc. is always provided except for the cases stipulated above.<br>(5). Procedure for approving not to stop the use, etc. according to the exceptional provisions is established, and approval of a manager in charge is obtained when stopping the use, etc. is not carried out according to the exceptional provisions. |
| 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 questions 37 (a), (b), (c), (d) and (e).<br>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.<br>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?<br>38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?<br>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?<br>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? | 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.<br>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.<br>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.<br>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. | **5.1 (Rights of the individual concerning personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 17-19.<br><br>**5.2 (Procedure for satisfying the rights of the individual concerning personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.f)<br><br>**5.3 (Making the matters concerning personal information subject to disclosure widely known)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.d)<br><br>**5.6 (Correction, addition, or deletion of personal information subject to disclosure)**<br><br>Reshown, see "Relevant Program Requirement" of Question 1.f)<br><br>**5.7 (Veto of use or provision of personal information subject to disclosure)**<br><br>Reshown, see "Relevant Program Requirement" of Question 37. |

**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 (*to be answered by the Applicant*)** | **Assessment Criteria (*to be verified by the Accountability Agent*)** | **Relevant Program Requirement** |
|---|---|---|
| 39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe.<br>• Internal guidelines or policies (if applicable, describe how implemented) _____<br>• Contracts _____<br>• Compliance with applicable industry or sector laws and regulations _____<br>• Compliance with self-regulatory applicant code and/or rules _____<br>• 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. | **1.3 (Privacy policy)**<br>Reshown, see "Relevant Program Requirement" of Question 1.<br>**2.2 (Laws, guidelines, and other codes stipulated by the state)**<br>Reshown, see "Relevant Program Requirement" of Question 7.<br>**2.5 (Internal regulations)**<br>Reshown, see "Relevant Program Requirement" of Question 8.<br>**4.3 (Supervision of employees)**<br>Reshown, see "Relevant Program Requirement" of Question 29.<br>**4.4 (Supervision of trustees)**<br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |
| 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.<br>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.<br>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. | **2.4 (Resources, roles, responsibility, and authorities)**<br>Representative of the applicant business entity shall prepare indispensable resources for establishing, implementing, maintaining, and improving its personal information protection management system. The resources shall fulfill the following conditions.<br>(1). Role and authority of each staff member are determined clearly and documented.<br>(2). Role, responsibility and authority of each staff member are determined clearly.<br>(3). A personal information protection manager is appointed from within the entity by the representative. A personal information protection auditor is appointed from within the entity by the representative; and auditors as defined by the Companies Law shall not take part in the system. The personal information protection manager is not the same person as the personal protection auditor.<br>(4). The role and authority of each staff member are informed to every staff member.<br>(5). The personal information protection manager is obliged to report on the operational status of the personal information protection management system to the representative of the entity in order to provide a basis for reviewing and improving the personal information protection management system; and the reporting is conducted. |
| 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:<br>1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR<br>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<br>3) A formal complaint-resolution process; AND/OR<br>4) Other (must specify).<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle. | **8. (Responses to complaints and consultation)**<br>The applicant business entity shall establish and maintain a procedure and system for implementing proper and prompt actions when receiving complaints from an individual and undertaking consultation with the individual. The following conditions regarding the issue shall be fulfilled.<br>(1). Procedures for accepting and appropriately and promptly responding to complaints from an individual and undertaking consultation with the individual with regard to the handling of personal information as well as the personal information protection management system of the entity are established.<br>(2). Person to be contacted for complaints and requests for consultation is clearly identified.<br>(3). Complaints and requests for consultation are accepted and responded in accordance with the procedures.<br>(4). The procedures for accepting complaints and requests for consultation are functioning, and responses are made promptly.<br>(5). Procedure for approving the content of the responses to be made to the individual is established, and the business is conducted accordingly while approval of a manager in charge regarding the content of the responses is obtained.<br>(6). Procedure for reporting on the details of complaints and consultation and the results of the responses thereto to |
| 42. Do you have procedures in place to ensure individuals receive a timely response to their | 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. | |

| | | |
|---|---|---|
| complaints? | Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle. | representative of the entity is established, and the reporting is conducted accordingly. |
| 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. | **1.3 (Privacy policy)**<br>Reshown, see "Relevant Program Requirement" of Question 1.<br>**8. (Responses to complaints and consultation)**<br>Reshown, see "Relevant Program Requirement" of Question 41-42. |
| 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.<br>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. | **6.(Training of employees)**<br>Reshown, see "Relevant Program Requirement" of Question 29. |
| 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.<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle. | **2.2 (Laws, guidelines, and other codes stipulated by the state)**<br>Reshown, see "Relevant Program Requirement" of Question 7.<br>**2.5 (Internal regulations)**<br>Reshown, see "Relevant Program Requirement" of Question 8.<br>**6.(Training of employees)**<br>Reshown, see "Relevant Program Requirement" of Question 29. |
| 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)?<br>• Internal guidelines or policies<br>• Contracts<br>• Compliance with applicable industry or sector laws and regulations<br>• Compliance with self-regulatory applicant code and/or rules<br>• Other (describe) _____ | Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described.<br>Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle. | **4.2 (Security control measures for personal information)**<br>Reshown, see "Relevant Program Requirement" of Question 10-12.<br>**4.4 (Supervision of trustees)**<br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |
| 47. Do these agreements generally require that personal information processors, agents, contractors or other service providers:<br>• Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement?<br>• Implement privacy practices that are | The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met. | |

| | | |
|---|---|---|
| substantially similar to your policies or privacy practices as stated in your Privacy Statement?<br>• Follow instructions provided by you relating to the manner in which your personal information must be handled?<br>• Impose restrictions on subcontracting unless with your consent?<br>• Have their CBPRs certified by an APEC accountability agent in their jurisdiction?<br>• Notify the Applicant in the case of a breach of the personal information of the Applicant's customers?<br>• Other (describe) _____ | | |
| 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. | The Accountability Agent must verify the existence of such self-assessments. | |
| 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.<br>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. | |
| 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:<br>(1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and<br>(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. | **3.8 (Measures concerning provision of personal information)**<br><br>Reshown, see "Relevant Program Requirement" of Question 10.-12. |